Titre: Title:	Hameçonnage bancaire : un cadre d'analyse et de réduction de risque de victimisation
Auteur: Author:	Jude Jacob Nsiempba
Date:	2017
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Nsiempba, J. J. (2017). Hameçonnage bancaire : un cadre d'analyse et de réduction de risque de victimisation [Ph.D. thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/2937/

UNIVERSITÉ DE MONTRÉAL

HAMEÇONNAGE BANCAIRE : UN CADRE D'ANALYSE ET DE RÉDUCTION DE RISQUE DE VICTIMISATION

JUDE JACOB NSIEMPBA

DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION

DU DIPLÔME DE PHILOSOPHIAE DOCTOR

(GÉNIE INDUSTRIEL)

DÉCEMBRE 2017

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse est intitulée :

HAMEÇONNAGE BANCAIRE : UN CADRE D'ANALYSE ET DE RÉDUCTION DE RISQUE DE VICTIMISATION

présentée par : NSIEMPBA Jude Jacob

en vue de l'obtention du diplôme de : Philosophiae Doctor

a été dûment acceptée par le jury d'examen constitué de :

M. ROBERT Jean Marc, Doctorat, président

Mme DEMARCELLIS-WARIN Nathalie, Doctorat, membre et directrice de recherche

M. FERNANDEZ M. José, Ph. D, membre et codirecteur de recherche

M. TRÉPANIER Martin, Ph. D, membre

M. BÉGIN Guy, Ph. D, membre externe

DÉDICACE

«Au bout de la patience, il y a le ciel»

Proverbe africain

À vous, mes parents, vous qui m'avez transmis le goût du travail acharné, la persévérance et la résilience, je vous dédie aujourd'hui ma réussite.

À mon épouse, ton amour, ta confiance indéfectible et ta présence dans ma vie me réconfortent et donne la force de continuer. Ce travail est un témoignage de mon attachement et de mon amour.

À mes enfants, Aïsha, Safi et Ken, votre existence m'a transformé, votre présence me comble de bonheur, je vous dédie ce fruit de l'effort en espérant qu'il vous inspirera.

À tous mes frères et sœurs, je vous prie de trouver dans ce travail l'expression de mon estime.

À toute ma grande famille, je vous prie d'accepter toute ma gratitude.

REMERCIEMENTS

Les mots ne suffisent pas pour exprimer ma profonde gratitude à Nathalie Demarcellis-Warin, ma directrice de recherche. Vos connaissances et votre expertise pour des questions économiques et de gestion du risque, votre énergie et vos multiples idées ont toujours rendu nos échanges très riches et constructifs. Je resterai toujours marqué par votre grande générosité et votre bonne humeur contagieuse.

À José M. Fernandez, mon co-directeur de thèse, j'exprime ma reconnaissance d'abord pour m'avoir conseillé ce sujet de recherche et, ensuite d'avoir accepté de diriger mes travaux de recherche. Chaque moment passé dans votre bureau était un moment de questionnement suivi de remise en cause des pistes de recherche mais surtout d'apprentissage intensif. Ces moments m'ont aidé à commencer et à continuer ce travail.

Je remercie chaleureusement et sincèrement Serge Alalouf pour ses conseils, ses encouragements et sa disponibilité pour toute question relative aux analyses statistiques. Serge, votre posture critique a contribué à façonner ma rigueur dans l'analyse des données.

À tous les experts en sécurité informatique qui ont accepté de participer à notre enquête sur les contremesures de sécurité, je vous suis sincèrement reconnaissant d'avoir consenti à mettre votre expertise et votre expérience au service de ce travail de recherche.

Je remercie bien évidemment ma famille, à qui je dois tellement. Merci infiniment à Aline, Safi, Aïsha et Ken d'être à mes côtés.

Je suis reconnaissant également envers mes amis, mes frères et sœurs de m'avoir aidé et écouté dans les moments de doute, notamment Étienne-François Mouajou, qui sait si bien me conseiller et me changer les idées, mais aussi à Raissa Nkemni, Djoumessi Laetitia et Alain Hounang.

À tous ceux et celles qui m'ont permis de commencer, de poursuivre et de finir ce travail, je dis merci !

RÉSUMÉ

La fraude bancaire, tout particulièrement celle qui implique l'hameçonnage, reste un enjeu majeur de la relation qu'entretiennent les banques avec leurs clients. Les statistiques croissantes sur les montants dérobés des comptes des victimes et la multiplicité des contremesures, des organismes nationaux et des coalitions multinationales d'entreprises qui luttent contre ce fléau en sont deux indicateurs de l'étendue du phénomène. Ce constat nous a amenés à aborder dans cette thèse, les questions des facteurs de risque de victimisation et des améliorations à apporter aux contremesures afin d'en diminuer les impacts.

A été étudiée en premier, la question de savoir quels sont les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire. Nous avons répondu à cette question en proposant un ensemble cohérent de quatre éléments sur lesquels doit s'appuyer toute définition de la victimisation par hameçonnage bancaire, notamment, l'action posée, l'objet utilisé, les présumés victimes et la nature des préjudices subis par lesdites victimes. Sur la base de ces éléments, nous avons défini trois formes de victimisation : la tentative d'hameçonnage, l'infection et la fraude.

Prenant appui sur ces trois formes de victimisation, nous avons développé un modèle de régression logistique pour analyser les données d'une vaste enquête canadienne (Enquête ESG, 2009) sur la victimisation en ligne afin d'identifier et classer hiérarchiquement les facteurs clés de risque de tentative d'hameçonnage, d'infection et de fraude (cf. Tableau 5.1). Il en ressort que les comportements à risque en ligne, de même que le manque de formation de base en sécurité et de sensibilisation aux menaces sont les catégories ayant le plus d'importance dans l'explication de la victimisation par tentative d'hameçonnage et par infection. Quant aux facteurs qui contribuent à la fraude (retrait de l'argent des comptes des victimes), les données de l'enquête ESG 2009 ne permettant pas d'étudier le processus de monétisation - manque de données sur le marché noir des renseignements volés -, nous avons développé un modèle théorique pour étudier les comportements de deux acteurs de ce marché noir : le fraudeur et la mule. Pour ce faire, nous avons appliqué la théorie du choix rationnel développée en économie. Aussi, les fonctions d'utilité classique de type CRRA (Constant Relative Risk Aversion) et de type CARA (Constant Absolute Risk Aversion) ont été utilisées pour étudier le comportement du fraudeur vis-à-vis du risque. Enfin, pour tester notre modèle théorique, nous avons exploité des données colligées des forums clandestins.

Les résultats de simulation de ce modèle révèlent que six facteurs ont une influence, à des degrés divers, sur le processus de monétisation. Il y a le revenu anticipé du fraudeur, l'intensité du niveau des mesures de sécurité mises en place par les banques, la commission versée à la mule, le prix du renseignement, la richesse initiale du fraudeur et la probabilité de se faire arrêter.

Afin d'évaluer la pertinence de notre modèle théorique pour répondre à notre question de recherche sur les facteurs clés de risque de victimisation, une enquête basée sur un échantillon par choix raisonné a été menée auprès de dix-sept experts en sécurité informatique. Les résultats de cette enquête confirment que deux des six facteurs déterminés par notre modèle théorique ont une grande importance dans le processus de monétisation. Il s'agit du revenu anticipé du fraudeur et du niveau de mesures mises en place par les banques. Deux autres facteurs que nous n'avons pas mesurés dans notre modèle, faute de données et de métriques, ont été retenus par les experts comme étant des facteurs ayant des effets prépondérants sur la décision de monétiser ou non un renseignement volé : la qualité du renseignement et le temps écoulé entre le vol du renseignement et le retrait de l'argent du compte de la victime.

Dans la même enquête, nous avons demandé aux experts de proposer des améliorations à apporter aux contremesures actuelles afin de réduire les risques de victimisation inhérents aux facteurs que nous avons déterminés. L'analyse des réponses des experts a permis d'adresser vingt-cinq recommandations aux pouvoirs publics, à l'utilisateur final, aux entreprises, aux développeurs de solutions de sécurité et aux organismes qui luttent contre l'hameçonnage bancaire.

Le modèle micro-économique que nous avons proposé est la principale contribution théorique de cette recherche. Quant à la principale contribution pratique, elle a été de proposer, en se basant sur les avis des experts, des améliorations à apporter aux contremesures actuelles afin de réduire, le cas échéant, le risque d'hameçonnage bancaire.

Cette recherche a toutefois quelques limites, notamment l'asymétrie d'information dans un marché noir de renseignements bancaires et le nombre limité des experts de l'enquête.

Il serait intéressant à l'avenir de prendre en compte l'asymétrie d'information dans l'analyse du marché noir et de valider le modèle conçu avec plus de données empiriques colligées des forums, des banques et auprès des experts en sécurité informatique.

ABSTRACT

Banking Fraud, specifically one which involves phishing, remains a major issue in the relationship that banks maintain with their clients. The rising statistics on the amounts stolen from victims' accounts as well as the multiplicity of countermeasures, the national organisations and the coalition of multinational businesses that fight against the plague, are two indicators of the extent of this phenomenon. This observation led us to examine in this thesis, the questions of victimisation risk factors and the improvements that can be made to countermeasures in order to diminish the impacts of phishing.

We first examined the question of determining the necessary and sufficient elements required to define victimisation by banking phishing. We have answered this question by proposing a coherent ensemble of four elements on which any definition of victimisation by banking phishing must repose. These include the action, the objects used, the presumed victims and the nature of the prejudices suffered by said victims. On account of these elements, we have defined three forms of victimisation: phishing attempts, infection and fraud.

On the basis of three forms of victimisation, we have developed a logistic regression model to analyse the data from an extensive Canadian investigation into online victimisation; in order to identify and hierarchically classify the key risk factors of phishing attempt, infection and fraud (Table 5.1). It appears that risky online behaviours, as well as the lack of basic training in security and threat sensitisation are the most important categories in the explanation of victimisation by attempt at phishing and by infection. As it related to factors that contribute to fraud (money withdrawal from victims' accounts), the data from the ESG 2009 investigation does not allow for a study of the monetisation process – lack of data on the black market of stolen information. We have developed a theoretical model to study the behaviours of two players in the black market: the fraudster and the mule. To carry this out, we applied the rational choice theory developed in economics. Also, the classical utility functions of the CRRA (Constant Relative Risk Aversion) and CARA (Constant Absolute Risk Aversion) varieties are used to study the behaviour of the fraudster vis-à-vis risk. Finally, to test our theoretical model, we took advantage of the data gathered from clandestine sites.

The results of the simulation of this model revealed that six factors influence, to different extents, the monetisation process. There is the anticipated revenue by the fraudster, the intensity of the level

of security put in place by the banks, the commission paid to the mule, the price of the information, the initial wealth of the fraudster and the probability of getting caught.

To evaluate the pertinence of our theoretical model in answering our research question on the key risk factors of victimisation, an investigation based on the rational choice sample has been performed among seventeen experts in information security. The results of this investigation confirmed that two out of six factors determined by our theoretical model have significant influence on the monetisation process. These include the anticipated revenue by the fraudster and the level of measures put in place by banks. Two other factors that we have not measured in our model, due to a lack of data and metrics, have been retained by the experts as factors having dominating effects on the decision to monetise or not stolen information: the quality of the information and the time elapsed since the theft as well as the withdrawal of money from the account by the victim.

In the same investigation, we have asked experts to suggest improvements that can be made to the actual countermeasures in order to reduce the inherent victimisation risks that we have determined. The analysis of the experts' responses has enabled us to provide twenty-five recommendations to authorities, the final user, businesses, security solutions developers and organisations that fight against banking phishing.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ANOVA	Analyse de la variance
APWG	Anti-Phishing Working Group
BOLETO	Terme portugais pour désigner un Ticket « Système de paiement utilisé au Brésil pour virer de l'argent, payer diverses choses en ligne »
BTAP	Protocole d'authentification des transactions biométriques
CA	Autorité de certification
CAFC	Centre Anti-fraude du Canada
CARA	Constant Absolute Risk Aversion
CER	Comité d'éthique de la recherche
CHAT	Messagerie instantanée
CRRA	Constant Relative Risk Aversion
DNS	Domain Name System
DNSBL	Domain Name System Black List
ESG	Enquête Sociale Générale
FBI	Federal Bureau of Investigation
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IC3	Internet Crime Complaint Center
IPAO	Interview en Personnes Assistés par Ordinateur
ITAO	Interviews Téléphoniques Assistées par Ordinateur
NW3C	National White Collar Crime Center
OTP	Codes à usag e unique

RIA	Rich Internet Application
SMS	Short Message Service
SSL/TLS	Secure Sockets Layer and Transport Layer Security
URL	Uniform Resource Locator
USPTO	United States Patent and Trademark Office
VPN	Virtual Private Network

LISTE DES ANNEXES

CHAPITRE 1 INTRODUCTION

La fraude[1] bancaire par hameçonnage - c'est-à-dire, le vol des renseignements bancaires par des techniques d'hameçonnage et leur conversion en argent ou biens et services - est en constante croissance depuis plusieurs années et le phénomène ne semble pas s'estomper. Bien au contraire, il est devenu une pratique répandue chez les escrocs du web (Rémillard, 2013) en raison de l'utilisation accrue des réseaux sociaux, du commerce en ligne, des appareils mobiles (Kritzinger & von Solms, 2010; Hille, Walsh, & Cleveland, 2015) et des solutions «cloud» pour stocker et gérer les données sensibles. Il suffit, pour s'en convaincre, de taper les termes «bank», «fraud», «Scam» et «phishing» dans Google ou dans Google Scholar. On obtient près d'un million de résultats dans Google et 10 800 dans Google Scholar. C'est dire à quel point le sujet est importante sur Internet et suscite l'intérêt des chercheurs et des organismes qui luttent contre l'hameçonnage. Parmi ces organismes, il y a l'Anti-Phishing Working Group (APWG) qui a publié dans son rapport de 2017 (APWG, 2017) que plus de 91% de toutes les attaques par hameçonnage en 2016 ont ciblé cinq types d'industries notamment, les institutions financières, les hébergeurs de données de type «cloud», les hébergeurs web, les services de paiement en ligne et les services e-commerce. Ce chiffre de 91% constitue une augmentation de 33% en moyenne par type d'industrie par rapport à 2015. Une augmentation qui est, toutefois, anormalement élevée dans le cas des compagnies canadiennes qui ont connu, parmi les pays développés, la plus forte croissance d'hameçonnage en 2016, soit près de 237% selon le rapport 2017 de Phishlabs (Phishlabs, 2017), principalement dans le secteur des institutions financières, où le plafond de 444% a été atteint (Bouchard, 2017). Les marques de commerce ciblées par des campagnes d'hameçonnage ont atteint un record en 2016 de 380 en moyenne par mois, soit 13% plus élevé que l'année précédente.

En plus de prendre pour cible les entreprises et les marques de commerce, les fraudeurs visent les consommateurs qui se connectent sur Internet. Le rapport de 2015 du Centre Anti-fraude du Canada (CAFC, 2015) révèle que les pertes financières déclarées et liées à l'hameçonnage pour des

[1] Le terme *fraude* utilisé seul signifie dans ce document, retrait d'argent du compte d'une victime sans son autorisation.

victimes au Canada sont passées de 3,6M $ en 2013 à près de 11M $ en 2016, soit une augmentation de 306%.

D'autres statistiques tirées des rapports 2016 et 2017 de l'APWG montrent que le nombre de sites Internet détectés qui étaient dédiés aux attaques d'hameçonnage est passé de 393K en 2014 à 1,22M en 2016, soit une augmentation de 310%. Quant au nombre de domaines où résident ces sites, il serait de 170K en 2016, ce qui représente une augmentation de 23% par rapport à 2015.

Fait nouveau depuis mars 2016, 93% de tous les courriels d'hameçonnage comportaient un système de chiffrement de type «ransomware» selon un rapport publié par l'organisme Phishme Inc (PhishMe, 2016). Aussi, on remarque une augmentation des types de cibles d'attaque. Les attaquants préfèrent de plus en plus s'en prendre aux systèmes de paiement en ligne comme PayPal, Boleto[2], Bitcoin (Jaeger, 2016), et aux entreprises qui gèrent les renseignements personnels.

Un autre indicateur, et non des moindres, de l'étendue du phénomène d'hameçonnage est la multiplicité, tant en Amérique que dans le reste du monde, des organismes nationaux et des coalitions multinationales d'entreprises de lutte contre ce fléau. Leur objectif : partager les informations et les savoir-faire afin de réduire, voire d'éliminer, le vol d'identité et la fraude qui résultent du problème croissant d'hameçonnage. Parmi ces organismes, citons, l'Anti-Phishing Working Group, *Internet Crime Complaint Center* (IC3) », partenaire du FBI[3] et du NW3C[4], l'organisme « The Coalition on Online Identity Theft », le site SCAMwatch[5], La *Federal Trade Commission* des États-Unis, l'organisme *The 419 Coalition Website* (Clearinghouse, 2003; The-419-Coalition, 2016; ACCC, 2017; IC3, 2017; Phishing-Initiative, 2017; USFTC, 2017).

En résumé, ce que nous pouvons retenir de ces chiffres, c'est que la fraude bancaire par hameçonnage :

- fait de plus en plus de victimes;

---

[2] Système de paiement utilisé au Brésil pour virer de l'argent, payer diverses choses en ligne.

[3] Federal Bureau of Investigation

[4] National White Collar Crime Center

[5] Site géré par la Concurrence et les Consommateurs de la Commission Australienne (ACCC)

- cause, à court terme, à l'échelle de l'individu, des pertes[6] et mine sa confiance[7] en Internet pour les transactions en ligne. Et, au niveau des entreprises, elle aurait pour effet de miner la confiance des clients et des titulaires de comptes à leur égard et de nuire à leurs images (Panda, 2011; Symantec, 2014);
- s'adapte de plus en plus aux nouvelles technologies de l'information (ex. SMS);
- cible de nouvelles sources économiques comme les entreprises qui gèrent des renseignements.

Au regard de ces chiffres en constante évolution et sachant que plus des deux tiers des Canadiens (68 %) utilisent Internet pour accéder aux services bancaires (ABC, 2017), nous trouvons qu'il est justifié de chercher à comprendre pourquoi malgré l'intensification des efforts des entreprises qui gèrent les renseignements et des organismes nationaux et des coalitions multinationales d'entreprises qui luttent contre ce fléau, malgré les services bancaires en ligne très sécurisés (Rémillard, 2013), ce phénomène ne s'estompe pas et les impacts chez les victimes sont toujours en hausse (Chaudhary, 2016). Une revue de la littérature révèle que plusieurs travaux de recherche ont abordé ce sujet au cours des dix dernières années. Nous avons regroupé ces travaux sous cinq rubriques différentes :

- les définitions;
- les techniques utilisées;
- les contremesures;
- le marché noir (forums clandestins);
- La victimisation.

Il appert de cette revue de littérature que la recherche dans ce champ d'activités a beaucoup évolué depuis près d'une décennie. Elle est passée d'une recherche purement technologique à une

---

[6] Statistiques Canada avance des chiffres de plusieurs dizaines de millions au Canada pour l'année 2011.

[7] Une étude de *Consumer Reports* menée en 2005 affirme que 9 adultes américains utilisateurs d'Internet sur 10 ont changé leurs habitudes relativement à Internet à cause du risque de vol d'identité et que, parmi ces utilisateurs, 30 % ont avoué avoir réduit de façon significative leur utilisation d'Internet. Aussi, 25 % des répondants déclarent ne plus acheter en ligne, tandis que 29 % de ceux et celles qui le font toujours déclare avoir diminué la fréquence de leurs achats.

recherche qui combine les aspects technologiques et humains (Chaudhary, 2016). Elle invite ainsi les chercheurs à emprunter des notions d'autres disciplines comme la criminologie, l'économie et les sciences sociales pour concevoir des contremesures qui prennent en compte à la fois les technologies de l'information et les aspects humains. Le défi majeur de la recherche est là et il grandit au fur et à mesure que les stratagèmes d'attaque deviennent plus raffinés et les techniques plus sophistiquées.

1.1 Problématique

Les statistiques présentées ci-dessus révèlent un certain nombre de problèmes. Tout d'abord, qu'il s'agisse du nombre d'attaques par hameçonnage ou du nombre de victimes ou encore de l'ampleur des impacts financiers engendrés par ces attaques, les chiffres recensés entre 2013 et 2016 ne cessent d'augmenter. Ce qui soulève un certain nombre de questions sur l'efficacité des contremesures mises en œuvre pour lutter contre ce phénomène. Selon Singh et al., aucune mesure technique, à elle toute seule, n'arrêtera complètement l'hameçonnage, en revanche, une combinaison de bonnes pratiques organisationnelles, d'utilisation correcte des technologies actuelles et de l'amélioration des connaissances et des enjeux de la sécurité peuvent réduire la survenance des attaques par hameçonnage et les pertes qu'elles engendrent (Singh, Somase, & Tambre, 2013). Or, la littérature consultée révèle qu'il y a un écart entre cette volonté de concevoir des solutions technologiques centrées sur l'humain et la pratique quotidienne. À titre d'exemple, le fait que les messages d'avertissement des «anti-phishing» ne soient pas adaptés à la dangerosité de la situation ou aux caractéristiques de l'utilisateur ne facilite pas leur compréhension (Mayhorn, Murphy-Hill, Zielinska, & Welk, 2015). Et, par conséquent, l'utilisateur a tendance à ignorer ces messages. Le défi ici, pour la recherche, est donc de travailler en amont pour que la solution technique intègre les préoccupations humaines. Pour cela, il faut étudier à fond les stratégies et techniques d'attaque qu'utilisent les hackeurs pour piéger leurs victimes, identifier les facteurs prédicteurs de fraude bancaire en utilisant des données d'enquête réelle de sorte à rendre les contremesures actuelles plus efficaces.

Ensuite, la littérature consultée étudie séparément l'attaque par hameçonnage et les marchés clandestins des produits de la cybercriminalité. Elle propose des taxonomies de l'hameçonnage fondées généralement sur une perspective de l'attaquant. Par exemple, Aleroud et Zhou fournissent une vue intégrée de l'hameçonnage qui comprend quatre dimensions: les médias de

communication, les environnements cibles, les techniques d'attaque et les contremesures (Aleroud & Zhou, 2017). Cette façon de caractériser l'hameçonnage n'établit pas le nécessaire pont entre le vol des renseignements et leur exploitation à des fins criminelles. Or, nous pensons que ce sont deux facettes complémentaires de la même industrie, celle de la fraude bancaire par hameçonnage car on a d'un côté, les activités qui contribuent au vol de renseignements et, de l'autre, celles qui exploitent ces renseignements à des fins criminelles. Le nécessaire pont est la victime. C'est elle qui subit le préjudice. Que ce soit lorsqu'elle reçoit des spams (hameçons), ou lorsqu'elle se fait voler ses renseignements ou encore lorsqu'elle se fait soutirer de l'argent de son compte. En ce sens, il serait intéressant et novateur d'étudier le processus de monétisation des renseignements et d'intégrer les éléments de risque clés qui en découlent dans une taxonomie complète de l'hameçonnage en prenant en compte la perspective de la victime. Ce que nous n'avons pas trouvé dans la littérature consultée. Probablement pour deux raisons : parce qu'il est très difficile d'obtenir des données quantitatives sur les activités criminelles auprès des banques, des services de police ou dans des forums clandestins, mais aussi, parce que nous n'avons pas trouvé de modèles théoriques qui analysent les marchés clandestins afin de déterminer les facteurs clés qui influent sur le processus de monétisation.

1.2 Objectifs de la recherche

Dans ce contexte, la question principale à laquelle cette recherche tente de répondre est de savoir si un cadre d'aide à la lutte contre l'hameçonnage bancaire auquel différents acteurs vont recourir pour réduire le risque de victimisation est possible.

Les différents travaux de recherche que nous avons consultés sur le sujet ont révélé qu'un tel cadre n'a pas encore été développé notamment, en raisons de certaines limites législatives, technologiques, administratives ainsi que celles inhérentes à la formation et à la sensibilité des utilisateurs aux enjeux de sécurité.

L'examen de ces limites a permis d'identifier les sous-questions de recherche clés suivantes :

Q1. Quels sont les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire ?

Q2. Quels sont les facteurs clés de risque de victimisation par hameçonnage bancaire ?

Q3. Quelles améliorations peut-on apporter aux filtres anti-hameçonnage afin de réduire les taux d'erreurs (ex. faux positifs ou faux négatifs) ?

Q4. Comment rendre les navigateurs plus sécuritaires à l'encontre des pirates ?

Q5. Un cadre juridique contraignant visant à favoriser l'échange des listes noires entre partenaires à l'intérieur d'un même pays et avec d'autres pays réduirait-il le temps de mise à jour de ces listes ?

Q6. Quelle est l'importance accordée aux formations en sécurité et aux campagnes de sensibilisation sur les menaces dans les organisations ?

Q7. Comment peut-on améliorer les formations et les campagnes de sensibilisation aux enjeux de sécurité?

Pour répondre à notre question centrale, nous nous sommes fixé comme objectif de proposer un cadre d'analyse et de réduction de risque d'hameçonnage bancaire. Cet objectif général se décline en quatre sous-objectifs :

1. proposer un cadre de définition de la victimisation par hameçonnage;
2. analyser
    - le comportement de l'internaute à chaque étape importante du processus de l'hameçonnage bancaire afin d'identifier les facteurs clés qui contribuent à sa victimisation;
    - le marché noir des renseignements bancaires afin d'identifier les facteurs clés de monétisation des renseignements;
3. valider les résultats d'analyse avec des données d'enquête réalisée auprès des experts en sécurité informatique;
4. formuler des recommandations d'améliorations à apporter aux mesures de lutte contre l'hameçonnage bancaire.

1.3 Méthodologie de recherche

Pour atteindre ces objectifs, une démarche méthodologique à la fois exploratoire et explicative est suivie. Tout d'abord, nous effectuons une revue de littérature basée sur les thèmes et mots clés issus de notre question principale. Cette revue permet de dresser un portrait de l'hameçonnage bancaire, d'identifier les insuffisances des solutions de lutte proposées dans la littérature, d'en faire une synthèse et d'émettre des hypothèses de recherche.

Ensuite, une étude explicative utilise les données de l'Enquête Sociale Générale (ESG) de Statistique Canada sur «les incidents auto-déclarés de victimisation sur Internet au Canada» de

2009 pour confirmer des hypothèses relatives aux facteurs clés qui contribuent à l'hameçonnage bancaire. Troisièmement, à défaut de disposer des données empiriques sur les marchés noirs qui permettraient de faire une analyse des facteurs qui contribuent à la monétisation, nous avons développé un modèle microéconomique théorique pour analyser ce marché en nous inspirant de ce qui se fait dans le marché de la drogue (Kopp, 1992; Deffains & Kopp, 2014) et du marché de contrebande et de la fraude documentaire (Daubrée, 1994). Pour tester ce modèle, des données publiées par Candid Wueest dans le rapport de Symantec 2015 (Wueest, 2015) sont utilisées.

Quatrièmement, une enquête basée sur un échantillon par choix raisonné a été menée auprès d'experts et de gestionnaires en sécurité afin de valider le modèle théorique de monétisation proposé au chapitre 6.

Et, finalement, nous avons exploité les réponses de l'enquête que nous avons réalisée auprès des experts pour proposer des améliorations à apporter aux les contremesures de sécurité.

1.4 Plan de la thèse

Le plan de cette recherche est structuré en neuf chapitres.

Le chapitre 2 est consacré à la revue de littérature sur la fraude bancaire par hameçonnage.

Nous y ferons un portrait de la fraude bancaire par hameçonnage afin de montrer l'ampleur et l'étendue de ce phénomène et dégager les hypothèses de recherche.

Le chapitre 3 présente l'approche méthodologique qui a été suivie. Deux méthodes d'enquête de collecte de données y sont présentées. L'une, effectuée par Statistique Canada au moyen d'interviews téléphoniques assistées par ordinateur (ITAO) dans les dix provinces canadiennes et, l'autre, réalisée dans le cadre de cette recherche au moyen de questionnaires administrés à des experts et gestionnaires en sécurité de plusieurs institutions et entreprises canadiennes. Les méthodes d'analyses statistiques utilisées et les notions micro-économiques utilisées pour développer le modèle théorique y sont présentées.

Le chapitre 4 propose un cadre de définition de la victimisation par hameçonnage bancaire et, pour chaque forme de victimisation identifiée, nous étudions les facteurs de risque qui s'y rapportent avant de formuler les hypothèses de recherche en lien avec nos questions de recherche posées au chapitre 1.

Le chapitre 5 présente un modèle de régression logistique binaire que nous avons développé pour analyser les facteurs de risque multiples et pour déterminer, parmi ces facteurs, ceux qui permettent de prédire la victimisation.

Le chapitre 6 présente un modèle micro-économique théorique d'équilibre partiel qui analyse le comportement du fraudeur au cours de l'activité de monétisation des renseignements bancaires sur les cybermarchés clandestins. Les fonctions d'utilité classique de type CRRA (Constant Relative Risk Aversion) et de type CARA (Constant Absolute Risk Aversion) sont utilisées pour étudier le comportement du fraudeur vis-à-vis du risque.

Le chapitre 7 présente les résultats d'une enquête basée sur un échantillon par choix raisonné qui a été menée auprès de 17 experts en sécurité informatique dans la grande région de Montréal afin de colliger leurs avis, à la fois, sur les facteurs qui influent sur le marché noir des renseignements bancaires et sur l'efficacité des mesures à prendre pour lutter contre l'hameçonnage bancaire. Et, compléter ainsi les résultats de l'étude exploratoire.

Le chapitre 8 présente les recommandations que nous avons formulées sur les améliorations à apporter aux contremesures de sécurité. Ces recommandations découlent de nombreuses années d'expériences en tant qu'architecte des systèmes TI[8] et analyste en sécurité informatique, couplées aux suggestions des experts consultés lors de l'enquête.

Le chapitre 9 présente la réponse à la question principale de recherche. Les contributions scientifiques de ce travail, les limites de recherche et les enjeux futurs y sont aussi présentés ainsi que la conclusion finale.

[8] Technologie de l'information

CHAPITRE 2 REVUE DE LITTÉRATURE SUR L'HAMEÇONNAGE BANCAIRE

La fraude, selon Simmons, se produit lorsqu'un fraudeur (un individu ou organisation) fait intentionnellement une fausse représentation et lorsque la victime (un individu ou une organisation), en se fiant à cette représentation, subit des pertes d'argent, de biens ou autres dommages (Simmons, 1995). En ce sens, la fraude peut se faire sans utiliser des techniques d'hameçonnage. Par exemple, l'accès frauduleux au compte bancaire d'une victime peut se faire par des techniques classiques de vol de portefeuilles ou par chapardage de cartes nouvellement émises dans la boîte aux lettres. Et aussi, l'hameçonnage peut servir de stratagème pour obtenir des renseignements à des fins autres que la fraude. Exemple, un chef d'entreprise peut faire télécharger et installer un cheval de Troie (avec toutes les apparences d'un logiciel légitime) sur l'ordinateur des employés afin de les surveiller.

Cette précision étant faite, notre revue de littérature sur la fraude des produits et services bancaires par hameçonnage est circonscrite à un type de fraude bien précise, celle qui utilise les techniques d'hameçonnage pour faire des victimes. Ce type de fraude n'a été connu du grand public qu'en 2001 après que deux attaques survinrent contre le système de monnaie électronique e-Gold la même année (Arnaques, 2015). En réalité, les principes de l'hameçonnage étaient déjà connus puisqu'ils avaient été exposés lors de la conférence Interex de 1987 par Jerry Felix et Chris Hauck (Felix & Hauck, 1987). Mais, c'est à partir de 2004 que ce phénomène prend de l'ampleur avec des pertes financières inhérentes chiffrées environ à 929 millions de dollars US pour la seule période de mai 2004 à mai 2005 aux États-Unis (Kerstein, 2005). Et, depuis ce temps, les attaques par hameçonnage à des fins d'escroquerie ont considérablement augmenté dans le monde.

De 2005 à 2015, l'APWG[9] a enregistré une croissance de plus de 800% des campagnes[10] de courriels hameçonnées dont une grande partie vise les institutions financières. Les pirates

[9] Anti-Phishing Working Group Inc.

[10] Une campagne de messagerie électronique est un e-mail unique envoyé à plusieurs utilisateurs afin de les rediriger vers sur un site web d'hameçonnage spécifique.

informatiques professionnels et les organisations criminelles ont depuis investi le créneau de l'hameçonnage bancaire et près de la moitié des vols d'identités par hameçonnage en 2006 ont été commis par des groupes opérant dans le cadre du *Russian Business Network* basé à Saint-Pétersbourg (Krebs, 2007). Pendant cette même période, les environnements cibles vont se préciser. Les clients des banques, des réseaux sociaux, des entreprises qui gèrent les renseignements personnels et les systèmes de paiement en ligne comme PayPal, Boleto[11], Bitcoin sont privilégiées par les auteurs d'attaques d'hameçonnage (Jaeger, 2016). Et, le phénomène s'adapte de plus en plus aux nouvelles technologies de l'information (ex. SMS «*Smishing*», CHAT). La vaste revue de littérature que nous avons effectuée sur ce sujet a permis de regrouper les travaux en cinq thèmes différents, à savoir :

- les définitions;
- les techniques utilisées;
- les contremesures;
- le marché noir (ou forums clandestins);
- la victimisation.

Mais avant, voici la méthodologie que nous avons utilisée pour effectuer cette revue de littérature.

2.1 Méthodologie de la revue de littérature

Le sujet de notre thèse comporte deux axes principaux. Tout d'abord, nous étudions les facteurs qui influent sur la victimisation par tentative d'hameçonnage et par infection et, ensuite, nous construisons un modèle microéconomique pour analyser le marché noir des renseignements bancaires afin d'aider à déterminer les facteurs de fraude. Pour ce second axe, nous empruntons des notions du domaine microéconomique pour étudier le marché noir des renseignements volés par hameçonnage. Aussi, l'approche méthodologique de la revue de littérature reflète ce caractère multidisciplinaire.

[11] Système de paiement utilisé au Brésil pour virer de l'argent, payer diverses choses en ligne.

L'examen de la littérature a donc été effectué en deux étapes. La première étape couvre le thème de la fraude par hameçonnage, son historique, son ampleur, sa caractérisation et, le cas échéant, ses limites. Quant à la seconde étape, elle examine les modèles économiques qui ont été utilisés par le passé pour étudier le comportement des marchés noirs et spécifiquement celui des renseignements bancaires.

2.1.1 Étape 1 : La recherche sur la fraude bancaire par hameçonnage

Pour cette étape, nous nous sommes inspirés de la revue systématique que Lastdrager a réalisée pour atteindre une définition consensuelle de l'hameçonnage (Lastdrager, 2014). Nous avons consulté plusieurs bases de données, le point de départ étant bien sûr Google Scholar, d'où émane la plupart de nos références scientifiques, suivi de ProQuest et d'Emeraldinsight. Les ouvrages consultés proviennent des bibliothèques de l'École Polytechnique et de l'UQAM. Les statistiques utilisées sont extraites des rapports des sites des organismes suivants :

- Association des banquiers canadiens;
- Centre antifraude du Canada;
- l'Anti-Phishing Working Group (APWG);
- l'Internet Crime Complaint Center (IC3);
- Symantec Corporation;
- PhishMe Inc.

Les thèses de doctorat ont été examinées en premier afin de nous assurer de l'originalité de notre travail (cf. Tableau A.1). Les bases de données en ligne Proquest et Google ont été utilisées comme sources pour toutes les thèses de doctorat. Les mots-clés «*thesis*», «*phishing*», «*fraud*», «*bank*», «*victimization*» «*Black*» «*market*» et «*undergound*» ont été utilisés pour identifier les thèses pertinentes pour notre recherche. En tout, treize thèses et un mémoire sont présentés au Tableau 2.1. Parmi les thèses consultées, onze abordent les thèmes liés à l'hameçonnage, les deux autres thèses et le mémoire traitent des sujets inhérents à l'économie souterraine.

Ensuite, nous avons étudié plus de 232 références liées au thème de la fraude par hameçonnage ou hameçonnage bancaire (cf. Tableau A.2). De ce nombre, les deux tiers étaient des articles de revues avec évaluation par les pairs et de conférences. Ils ont été privilégiés en raison du processus

rigoureux d'acceptation dont ils font l'objet dans les revues et actes des conférences. Les livres ont été peu exploités, en revanche, les articles tirés des sites web spécialisés et des médias publics sur le sujet ont été aussi d'une grande utilité car les informations qu'ils hébergent sur le sujet sont d'actualité et assez diversifiées. Pour sélectionner ces articles, nous avons utilisé les mots clés «*phishing*» «*fraud**», «*bank*», «*victimization*» dans *Google Scholar*. On a obtenu 2060 résultats, puis, en raffinant notre recherche par intervalle de temps, nous avons obtenu les résultats suivants :

Tableau 2.1 : Références sur la fraude par hameçonnage

Source	**Mots clés**	**Période**			
Google Scholar	"phishing", "fraud*", "bank", "victimization"	1987 à 2000	2001 à 2004	2005 à 2010	2011 à 2017
Résultats	2060	6	25	709	1320
Références retenues	144	3	4	65	72

Le Tableau 2.1 présente les références retenues pour cette revue de littérature. Ces références y sont regroupées selon le titre de l'article et le thème de classification que nous avons énoncé ci-dessus. En tout, 144 références ont été étudiées.

Afin de compléter cette première étape de la revue de littérature, nous avons aussi fait une recherche des brevets relatifs à notre sujet sur le site de l'office de la protection intellectuelle du Canada et de celui de «*The United States Patent and Trademark Office* (USPTO)». La recherche avec les mots clés «phishing», «fraud*» et «bank» a produit deux résultats sur les brevets au Canada et 567 sur les brevets américains. Le Tableau A.3 présente quelques-uns des brevets que nous avons sélectionnés et qui se rapportent à l'orientation de notre recherche.

2.1.2 Étape 2 : La recherche sur les modèles économiques et le marché noir

Pour la deuxième étape, nous avons choisi de circonscrire la revue de littérature au marché noir des ventes des produits et services bancaires en utilisant les mots clés suivants : «underground or black» and «*market*» and «*credential*» and «*economy*» and «*phishing*» and «*victim*» and *fraud* dans Google Scholar et Emeraldinsight. Ces bases de données ont été les deux sources principales. Les revues et les articles des conférences internationales ont été sélectionnés comme étant des

documents pertinents pour les mêmes raisons qu'à l'étape 1. Les documents avec les termes «phishing» et «fraud» dans leur titre d'article ont été sélectionnés pour la lecture rapide. Le Tableau 2.2 ci-dessous donne le résumé du résultat de cette recherche par mots clés.

Tableau 2.2 : Références sur les modèles économiques et le marché noir

Source	**Mots clés**	**Période**		
Google Scholar/ Emeraldinsight	"phishing", "fraud*", "bank", "victimization" "underground or black" "market", "credential*", "economy"	1968 à 2004	2005 à 2010	2011 à 2017
Résultats	500	4	113	383
Références retenues	77	5	38	34

2.2 Définitions

Le sujet que nous abordons dans cette recherche est très vaste et il y a eu, au fil des ans, beaucoup de travaux de recherche qui ont été menés. Il est donc important, avant même d'analyser ces travaux, de circonscrire notre champ d'action et de bien définir, à la lumière de la revue de littérature, les termes et les définitions que nous utiliserons dans ce travail.

Dans «fraude bancaire par hameçonnage», il y a d'abord le mot fraude. La définition la plus générale de la fraude que nous avons trouvée vient de Simmons (Simmons, 1995). Pour lui, la fraude survient lorsque tous les éléments suivants existent :

- un individu ou une organisation fait intentionnellement une fausse représentation sur un fait ou un événement important;
- la victime (la personne ou l'organisation à laquelle la représentation a été faite) croit en cette fausse représentation;
- la victime s'appuie et agit sur la base de la fausse représentation;
- la victime subit une perte d'argent et/ou des biens en raison de la dépendance et de la fausse représentation.

Il y a ensuite, l'expression «fraude bancaire». L'examen de la littérature montre qu'elle survient lorsque la fraude, telle que définie par Simmons, vise à obtenir de l'argent, des actifs, des crédits, des valeurs mobilières ou d'autres biens appartenant ou détenus par une institution financière, ou d'obtenir de l'argent des clients d'une banque (Legaldictionary, 2017). Une autre définition de la fraude bancaire que nous avons retenue vient de Ramsey et se formule comme suit : La fraude bancaire est une infraction pénale consistant à exécuter ou tenter sciemment d'exécuter un schéma ou un artifice pour frauder une institution financière ou pour obtenir des biens détenus par ou sous le contrôle d'une institution financière au moyen de prétentions, de représentations ou de promesses fausses ou frauduleuses (Ramsey, 2017).

Enfin, il y a dans notre titre de recherche le terme hameçonnage ou phishing en anglais. En raison de l'importance du phénomène auquel réfère ce mot dans ce travail, nous avons étudié à fond les différentes définitions trouvées dans la littérature. Nous vous présentons quatre de ces définitions dans les lignes qui suivent :

Définition 1 : (Chan, 2004)

Le «phishing» est une forme de fraude dans laquelle les victimes reçoivent de faux courriels prétendument envoyés par les banques leur demandant de fournir des informations personnelles sensibles à un site web de banque faussement accessible via un lien hypertexte intégré dans le courrier électronique.

Définition 2 : (Chawki, 2006)

Le «phishing» est l'acte d'envoyer un courrier électronique à un utilisateur en prétendant faussement être une entreprise légitime établie dans le but d'arnaquer l'utilisateur afin de lui soutirer les informations privées qui seront utilisées ensuite pour le vol d'identité.

Définition 3 : (Renaudin, 2011)

Le «phishing» est une contraction des termes anglais « fishing » (pêche) et « phreaking» (fraude informatique). Cette technique de fraude consiste à envoyer un e-mail non sollicité à une personne dans le but d'obtenir ses coordonnées confidentielles, le plus souvent ses données bancaires, en se faisant passer pour une société ou une institution financière connue afin de mettre en confiance le destinataire et, l'inciter à communiquer les informations sollicitées.

Definition 4: Anti-Phishing Working Group (2013)

L'hameçonnage est un mécanisme criminel utilisant à la fois l'ingénierie sociale et un subterfuge technique pour voler les données d'identité personnelle des consommateurs et les informations d'identification des comptes financiers. Les schémas d'ingénierie sociale utilisent les courriels falsifiés et de faux sites web conçus pour amener les consommateurs à divulguer des données financières telles que les noms d'utilisateur et les mots de passe en prétendant être des entreprises ou des organisations légitimes. Les systèmes techniques de subterfuges installent des produits criminels sur des ordinateurs pour voler directement les informations d'identification en utilisant souvent des systèmes pour intercepter les utilisateurs et en altérant les infrastructures de navigation locales pour diriger les consommateurs vers des sites web contrefaits.

Il ressort de l'analyse de ces définitions que trois concepts sous-tendent la fraude bancaire par hameçonnage. La fausse représentation dont parle Simmons fait référence au concept d'*usurpation* d'identité (Mihai, 2012) alors que la contrefaçon des sites web et la manipulation des courriels renvoient aux concepts de *dissimulation* et de *falsification* (Q. Ma, 2013a).

Enfin, il y a un autre élément dont on ne parle pas dans les quatre définitions que nous avons retenues et qui n'apparaît pas non plus de façon explicite dans notre titre de recherche mais que la revue de littérature a révélé comme étant un maillon essentiel qui complète la fraude par hameçonnage. C'est le concept de marché noir, c'est-à-dire un espace d'échange ou se transigent les produits et services bancaires issus de la fraude par hameçonnage (Hutchings & Holt, 2017).

2.3 Techniques utilisées

2.3.1 Mécanismes d'envoi de l'hameçon

Le moyen le plus usuel et le plus efficace d'envoyer, à « l'aveugle » ou de manière ciblée, l'hameçon (ou pourriel) est le courriel électronique (Chhikara, Dahiya, Garg, & Rani, 2013). Et, une des sources d'envoi les plus efficaces est le *botnet*[12] malveillant (Maggi, 2010). Un botnet peut comprendre plusieurs milliers d'ordinateurs infectés par un logiciel malveillant qui réalisent, pour

[12] Un botnet est un réseau de machines zombies contrôlées à l'insu de son utilisateur par un hacker qui s'en sert à des fins malveillantes.

le compte d'un « *hacker* », des attaques de toutes sortes, incluant des attaques d'hameçonnage bancaire. Le hacker envoie la commande aux machines infectées et celles-ci, à leur tour, envoient des pourriels en masse en utilisant des listes de pollupostage. Les listes d'adresses électroniques sont constituées en amont par des robots et selon un processus qu'on qualifie de « *Harvesting* », c'est-à-dire de découverte automatisée d'adresse publiée sur Internet (Abad, 2005).

2.3.2 Techniques d'usurpation

- La dissimulation « *Cloaking* »

C'est une technique qui permet de dissimuler la véritable adresse d'une page web visitée dans la barre de navigation (Trudel, Abran, & Dupuis, 2007). Elle se fait de trois façons. Soit en exploitant une vulnérabilité du navigateur, soit en plaçant un «pop-up» pour tromper la vigilance de l'internaute et faire croire à une autre adresse dans la barre du menu, soit en utilisant un jeu de «frame» en langage HTML.

- Usurpation « *Spoofing* »

Cette technique est utilisée pour se faire passer pour un autre. Le but, pour un attaquant, est de masquer son identité (ici, l'adresse IP) et d'usurper l'identité d'un autre ordinateur afin de tirer profit des privilèges de ce dernier (Kruck & Kruck, 2006).

2.3.3 Stratagème de l'hameçonnage

2.3.3.1 L'hameçon

L'hameçon en informatique désigne un message dont se sert un attaquant pour prendre sa victime (Costăchescu, 2012). Il existe différents types d'hameçon, notamment, les pourriels[13], les messages instantanés « *ou chat* », les fausses sollicitations sur les sites de réseaux sociaux, les SMS et les appels vocaux.

Dans le cas où l'hameçon est un pourriel, l'attaquant le crée de sorte à reproduire fidèlement le style de courriel, le logo, la bannière, le slogan de l'organisme dont le criminel veut en usurper

[13] Construit à partir des termes *poubelle* et *courriel*, le pourriel désigne le courriel non sollicité ou non souhaité [Office québécois de la langue française, mai 1997]. Ainsi définis, tous les pourriels ne conduisent pas forcément à l'hameçonnage. En revanche, il est le vecteur par excellence du hameçonnage classique.

l'identité. Il falsifie ensuite le champ expéditeur «De» du pourriel qu'il remplace par une adresse apparemment légitime (ex.. ibanking@ib.rbc.com). De plus, il s'assure que les autres éléments du pourriel qui font référence au site de l'organisme cible sont presqu'identiques aux éléments du site officiel. Pour cela, il utilise des techniques d'usurpation « *Spoofing* » et de dissimulation « *Cloaking* ».

Selon Smyth et al., le stratagème joue le rôle d'appât pour voler les renseignements des victimes. En règle générale, ce stratagème comprend trois éléments (S. Smyth & Carleton, 2011) : la demande de renseignements personnels, l'urgence d'agir et les liens vers des sites malveillants. Des sites qui, grâce aux techniques de plus en plus sophistiquées, ressemblent étrangement aux sites légitimes.

- Demande de renseignements personnels

La formulation de la demande de renseignements personnels se présente souvent comme une nécessité de l'organisme avec qui le client fait affaire (S. Smyth & Carleton, 2011) . À titre d'exemple, certains messages invoquent la nécessité de mettre à jour des informations sur les comptes bancaires alors que d'autres proposent des articles en vente sous forme d'enchères en ligne ou une assurance anti-fraude afin d'inciter la victime à effectuer des paiements sur des sites contrefaits et malveillants, et, en profiter pour colliger les renseignements personnels.

- Urgence d'agir

En ce qui concerne l'urgence d'agir, le stratagème tente de créer un caractère impératif qui incite le destinataire à répondre instantanément sans réfléchir. Par exemple, on retrouve dans certains messages des phrases comme « *si nous ne recevons pas ces informations dans xx heures, votre compte sera bloqué* ».

- Lien vers les sites ou numéros de téléphones fictifs/malveillants

Pour ce qui est des liens vers des sites contrefaits, les hackers utilisent des techniques des plus sophistiquées pour créer des sites trompeurs mais d'apparence légitime, si bien qu'il est très difficile pour un utilisateur non avisé de deviner si le site référencé est légitime ou pas (Hong, 2012). Un autre élément que l'on retrouve dans certains stratagèmes est le message de courtoisie émis à la fin de l'opération. En effet, pour éviter tout soupçon de fraude, certains faux sites émettent un message

rassurant et de remerciement à l'endroit de la victime. À titre d'exemple : « *La mise à jour des informations de votre compte s'est terminée avec succès, nous vous remercions pour la confiance que vous nous faites et vous assurons de tout mettre en œuvre pour vous donner entière satisfaction* » etc.

Le stratagème mise sur le fait que des utilisateurs préfèrent, pour se faciliter la tâche, cliquer sur un hyperlien plutôt que de taper au clavier l'adresse URL.

Dans le cas de l'hameçonnage vocal, Choi et al. soulignent la particularité du stratagème dans la formulation du message. Certains messages sont plus convaincants lorsqu'ils sont communiqués par voie orale. Et, pour d'autres, le fait que le message s'accompagne d'éventuels échanges téléphoniques est rassurant. Citons, à titre d'exemple, la nécessité de soumettre ou de corriger une déclaration de revenu ou, de façon plus spectaculaire, les enlèvements (kidnapping) de personnes.

2.3.4 Les variantes d'hameçonnage bancaire

2.3.4.1 L'hameçonnage par tromperie

Cette forme d'hameçonnage, encore connue sous le vocable d'hameçonnage par ingénierie sociale, peut être catégorisée en neuf sous types (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Mayhorn et al., 2015). Il y a :

1. l'hameçonnage par « *pièce jointe* »: il est caractérisé par l'envoi de courriel contenant une pièce jointe. Cette pièce peut être un formulaire à remplir ou un logiciel malveillant (logiciel espion ou un virus). Selon un rapport de Symantec (Symantec, 2014), 1 courriel sur 195 analysés contenait une pièce jointe malveillante, soit une augmentation de 16% par rapport l'année 2013;
2. l'hameçonnage par « *redirection* »: c'est la forme la plus courante d'hameçonnage. « *L'hameçonneur* » incite l'internaute à suivre des liens qui le redirige vers des sites malicieux. Ces sites utilisent des codes en JavaScript pour capter les informations (Jagatic et al., 2007).

3. Le « *Spear phishing*»[14] : c'est un type d'hameçonnage qui, à l'aide de courriels personnalisés ou de techniques d'ingénierie sociale, cible de façon précise une ou plusieurs éventuelles victimes et leur envoi un hameçon dans le but d'obtenir des renseignements personnels ou autres informations sensibles (Aleroud & Zhou, 2017; Aycock, 2007; Peterson, 2011).
4. Le «*in-session phishing*» : il survient pendant la visite normale d'un site de confiance sécurisé. Une fenêtre pop-up s'ouvre invitant l'internaute à y inscrire ses renseignements. Une fois les informations validées, l'instigateur de l'attaque peut les réutiliser. Ce type d'hameçonnage utilise des scripts Java qui déclenchent une action si le site de confiance est visité en même temps que le site contenant le script (Eisen, 2009).
5. L'hameçonnage vocale « *voice phishing* »: C'est un type d'hameçonnage qui utilise le téléphone pour persuader les victimes de leur dévoiler leurs renseignements personnels (Maggi, 2010). Le stratagème peut prendre deux formes. La première façon est d'envoyer un pourriel comme lors du hameçonnage classique et, au lieu que le criminel mette un hyperlien trompeur dans le pourriel, le pourriel fournit, par exemple, un numéro de téléphone du service à la clientèle de l'organisme dont on usurpe l'identité et où la victime présumée devrait appeler. La seconde façon est d'appeler la cible potentielle et lui demander d'appeler à un numéro de service où il devrait fournir ses renseignements pour éviter un supposé problème (K. Choi, Lee, & Chun, 2017).
6. L'hameçonnage « Quick Response Codes » : Il repose sur la substitution du Code QR présent sur une affiche par un autre (ex. en collant une autre étiquette par-dessus le code QR). La victime est alors redirigée vers un contenu malveillant (Kieseberg et al., 2010; Lerner et al., 2015).
7. L'hameçonnage de type « *pharming* » ou « *DNS poisonning* »: C'est une technique utilisée pour rediriger, grâce à un logiciel malveillant installé sur l'ordinateur de l'utilisateur à son insu, les adresses de sites web légitimes tapées au clavier vers les sites contrefaits. Elle exploite une vulnérabilité du navigateur web pour modifier le fichier « *Hosts*[15] » afin d'obliger le système à rediriger les requêtes s'adressant à un nom de domaine légitime (ex..

[14] Harponnage au Québec

[15] Le fichier *hosts* est consulté à chaque connexion à un site web, un peu comme un répertoire d'adresses

polymtl.ca) vers l'adresse IP du serveur web de « *l'hameçonneur* ». Une telle attaque est alors qualifiée d'attaque par usurpation du serveur (Milletary & Center, 2005; Gastellier-Prevost, 2011; K. Choi et al., 2017).

8. L'hameçonnage par mystification de domaine «*Domain Spoofing*» : il consiste à modifier les réglages du protocole TCP/IP afin d'envoyer à un serveur des paquets qui semblent provenir d'une autre adresse IP connue du pare-feu. Ce qui veut dire, par exemple, qu'en cliquant sur l'hyperlien du pourriel ou même en saisissant l'URL correctement dans le navigateur, l'utilisateur est réacheminé vers un site web falsifié alors que l'URL du site légitime s'affiche. L'utilisateur qui croit être sur le bon site rentre ses renseignements personnels et la suite est similaire aux autres cas de figure (Dhamija, Tygar, & Hearst, 2006).
9. Enfin, Felt. et Wagner 2011 expliquent qu'il y a l'hameçonnage par SMS[16] «SMiShing». Avec les nouvelles technologies mobiles, les messages texte sont devenus un moyen privilégié de communication entre utilisateurs du mobile et, de plus en plus, celui des hackers pour atteindre leurs cibles. Le principe reste le même que le courriel, toutefois, les interactions entre site web et les applications mobiles dans un écran limité physiquement crée souvent de la confusion et expose les utilisateurs au risque de confondre une application malveillante à une application mobile légitime. De plus, les systèmes d'exploitation et les navigateurs mobiles ne disposent pas d'indicateurs d'identité sécurisée pour les applications. Pour ces raisons, l'hameçonnage via les mobiles seraient en progression (Felt & Wagner, 2011). Mais, peu d'études le confirment pour l'instant.

2.3.4.2 L'infection par hameçonnage

Elle est caractérisée par l'introduction, suite à un clic sur un lien ou sur une pièce jointe ou encore suite à une visite d'un site malveillant, d'une porte dérobée « *backdoor* » dans un des logiciels de l'ordinateur de la victime (Hutchings & Holt, 2017). Cette porte dérobée exploite une faille de sécurité (ex. Adobe Flash - CVE-2011-0609) pour ouvrir un ou plusieurs ports sur l'ordinateur, ce qui transforme, à l'insu de l'utilisateur, le logiciel légitime en un logiciel contenant une malveillance

[16] Short Message Service

(ex. un cheval[17] de Troie). Le hacker utilise ce cheval de Troie pour prendre le contrôle de la machine et y injecter d'autres logiciels malveillants (ex. logiciel espion «spyware»). Ainsi, il peut capter les informations frappées au clavier «en utilisant un *keylogger*», les enregistrer dans des formulaires en ligne et les acheminer à un serveur distant. Il peut aussi détourner la session en cours en modifiant le fichier hôte ou la cache du DNS (*Domain Name System*). Les données recueillies sont ensuite décodées et exploitées à des fins malveillantes (Emigh, 2006).

Une autre technique d'hameçonnage par implantation de logiciels espions communément appelée technique du plan d'eau «*watering holes*» a vu le jour depuis 2011. Elle repose sur la notion de profilage. «L'*hameçonneur*» fait le profilage social des internautes et analyse les sites Internet fréquentés par sa cible. Ensuite, comme l'explique le rapport Symantec 2016, il trouve une faille de sécurité sur un de ces sites légitimes et y intègre un code malicieux. Puis, comme un prédateur qui attend sa proie près d'un plan d'eau sachant qu'elle devra tôt ou tard venir s'y abreuver, il va attendre que la victime visite à nouveau le site et en profiter pour installer un logiciel malveillant sur son ordinateur ou son appareil mobile et, le tour est joué (Affaires, 2014; Symantec, 2016).

La figure 2.1 qui suit résume l'ensemble des techniques recensées dans la littérature.

[17] C'est un logiciel malveillant d'apparence légitime qui permet au criminel d'avoir accès à l'ordinateur de l'utilisateur à son insu pour y installer d'autres programmes (ex. logiciel espion, « *spyware* »).

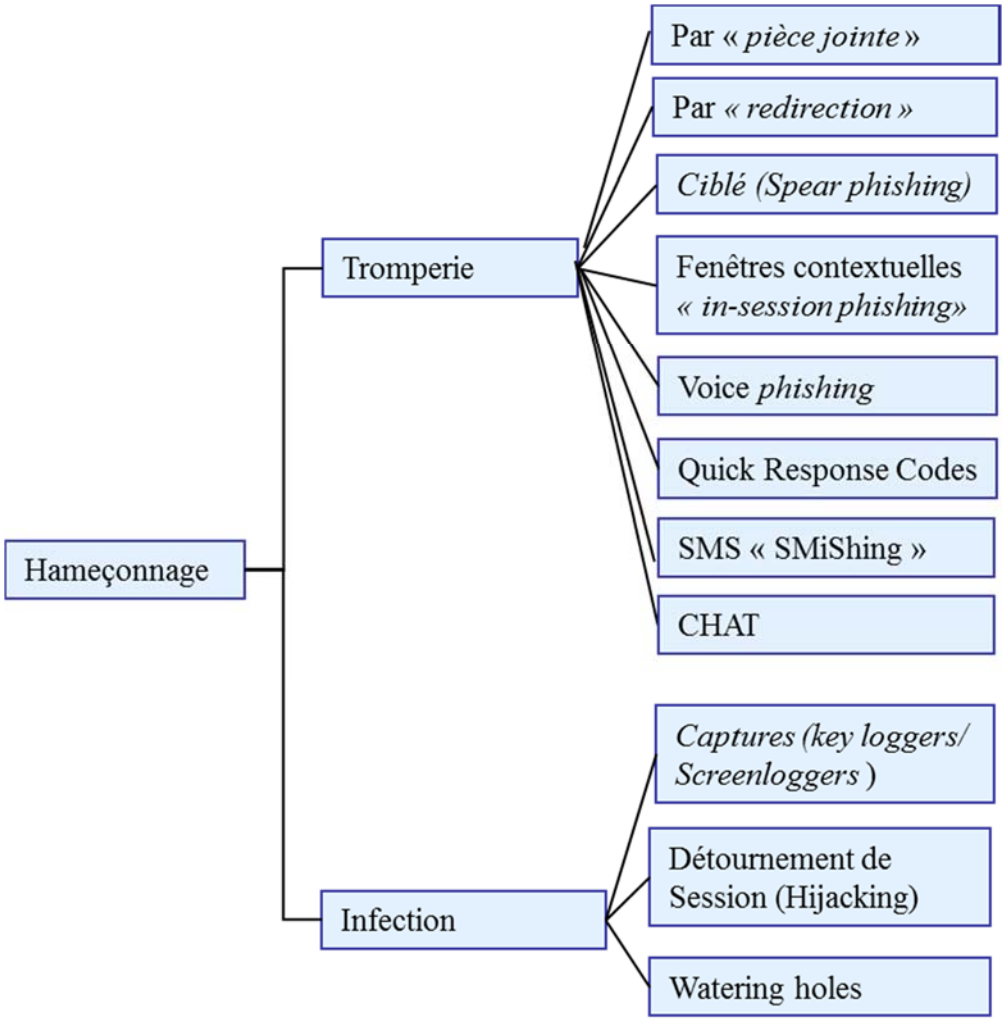


Figure 2.1 : Variantes et vecteurs d'hameçonnage

2.4 Contremesures

La revue de littérature sur les solutions de lutte contre l'hameçonnage bancaire est particulièrement riche. Afin de bien analyser tous les efforts de recherche qui ont été déployés par le passé et de poser les bonnes questions relatives aux raisons qui expliquent que malgré tout ce travail, la fraude par hameçonnage continue de croitre, nous avons regroupé toutes les contremesures tirées des documents consultés en cinq catégories :

- contremesures législatives;
- contremesures technologiques;
- contremesures administratives;
- contremesures éducatives et de sensibilisation;
- contremesures opérationnelles (blocage de cartes de crédit, etc.).

2.4.1 Contremesures législatives

L'examen de la littérature révèle qu'il y a, depuis le début des années 2000, une prise de conscience du danger que représente la cybercriminalité et qu'une législation spécifique a été développée à divers niveaux nationaux et internationaux pour lutter contre la fraude en ligne (Symantec, 2008). Par exemple, tous les pays du G8 se sont dotés d'un cadre général régissant les pourriels. Le Canada, pour sa part, a adopté en décembre 2010 la « LÉPI » (Robertson, 2011), la loi visant l'élimination des pourriels sur les réseaux Internet et sans fil. Cette loi protège les renseignements personnels et les documents électroniques. Cette loi vise aussi à promouvoir le commerce électronique tout en décourageant l'envoi de pourriels, le vol d'identité, l'hameçonnage, les logiciels espions, les virus et les réseaux de zombies de même que la publicité trompeuse en ligne. Aux États- Unis, c'est la CAN-SPAM Act[18] qui s'applique depuis 2004. Il s'agit de la loi américaine qui régit l'envoi de courriels commerciaux.

Dans leurs travaux, les auteurs Bainbridge, Larcom et al. et Granova et al. relèvent que la loi doit tenir compte des risques techniques actuels ainsi que des mesures prises pour les contrer (Granova & Eloff, 2005; Larcom & Elbirt, 2006; Bainbridge, 2007). Granova et al. (2005) ont mené une étude détaillée sur l'expérience d'hameçonnage et le cadre juridique disponible dans plusieurs pays. D'autres auteurs comme McNealy, Pinguelo et al. ont examiné les lois anti-hameçonnage existantes dans différents états américains ainsi que la législation fédérale. Ils concluent que l'arsenal juridique actuel est adéquat pour punir sévèrement les auteurs de «phishing» et dédommager les victimes de fraude par hameçonnage (McNealy, 2008; Pinguelo & Muller, 2011).

[18] "Controlling the Assault of Non Solicited Pornography and Marketing Act"

Dans son article, Umejiaku examine le cadre juridique qui réglemente l'accès public à l'information dans le cyberespace au Nigéria. Le document souligne également les lacunes inhérentes au système juridique nigérian. Sur la base des résultats obtenus, le document propose un certain nombre de recommandations. Il propose qu'en raison du développement rapide de la technologie, le droit et l'éthique devraient être combinés pour protéger la société de la menace de la cybercriminalité (Umejiaku, 2015).

Un autre article, celui de Larson et al., va plus loin en recommandant aux tribunaux d'examiner la possibilité de sanctionner à grande échelle. C'est-à-dire les «*hameçonneurs*», les fournisseurs d'accès Internet, les propriétaires de forums clandestins et les détenteurs de marques de commerce illégales (Larson, 2010). De telles sanctions inciteraient toutes les parties prenantes à participer activement à l'effort de lutte anti-hameçonnage. Guillaume Lovet dans son article souligne les défis judiciaires et éthiques du combat contre l'hameçonnage et recommande une coopération internationale et une harmonisation des infractions de la cybercriminalité des systèmes judiciaires transfrontaliers (Lovet, 2009).

2.4.1.1 Limite des contremesures législatives

À la lumière de ce qui précède, il appert que la fraude par hameçonnage fait intervenir de nombreux participants ayant des intérêts différents : utilisateurs, fournisseurs de navigateurs, développeurs, fournisseurs de serveurs web, hébergeurs de sites web, régulateurs et comités de normes, etc. Il n'est donc pas facile de parvenir à un accord opportun avec autant d'intervenants. Un cadre juridique qui intègre les considérations de tous ces intervenants est le principal défi de lutte contre l'hameçonnage (Dinna, Leau, Habeeb, & Yanti, 2008). Un défi d'autant plus difficile car aucune loi ne peut contraindre un utilisateur à prendre des dispositions pour se protéger (Smedinghoff, 2005). Toutefois, au niveau des organisations, la donne est différente puisqu'une entreprise peut mettre en place des mesures administratives contraignantes afin d'appliquer une telle législation.

2.4.2 Contremesures technologiques

Les références que nous avons consultées sur le sujet ont permis de regrouper les contremesures technologiques en six catégories :

- les filtres anti-hameçonnage;

- la gestion de barre d'outils et des mots de passe;
- les listes de restriction;
- les détecteurs de sites malicieux;
- l'authentification multiple;
- les fichiers de journalisation.

2.4.2.1 Les filtres anti-hameçonnage

Selon Viswanath et al., plus l'internaute reçoit des courriels, plus il est probable qu'il se fasse tromper (Vishwanath, Herath, Chen, Wang, & Rao, 2011). En utilisant les filtres anti-hameçonnage basés sur la classification automatique, on peut empêcher que les attaques n'atteignent les utilisateurs finaux. Pour cela, on peut configurer, en amont les filtres des serveurs et, en aval, les filtres des utilisateurs finaux afin de discriminer les courriels légitimes des courriels frauduleux (Del Castillo, Iglesias, & Serrano, 2007). Dans le même ordre d'idées, Chandrasekaran et al. proposent dans un article une technique pour discriminer les courriels légitimes des courriels illégitimes en utilisant les caractéristiques structurelles distinctes qui sont présentes dans le courriel. Cette solution a, par le passé, empêché un grand nombre de tentatives de vol d'identité. Toutefois, cela implique un travail colossal avec beaucoup de ressources pour un résultat mitigé car ces filtres ne permettent pas d'aller chercher les caractéristiques distinctives dans des courriels (Murphy, 2005). La nouvelle approche proposée dans l'article de Berghoz et al. apporte justement des éléments de réponse à ce problème en offrant l'apprentissage actif pour l'analyse des textes électroniques, des liens externes, la détection des logos intégrés ainsi que des indicateurs pour détecter la distorsion des contenus non perceptibles. Ce filtre conduit à de meilleurs résultats que l'approche par classification automatique (Bergholz et al., 2010). Fette et al. apportent des améliorations à la technique en proposant un filtre spécialisé appelé PILFER[19]. Ce filtre permettait d'identifier dans les courriels les patrons caractéristiques de certains types de menaces (Fette, Sadeh, & Tomasic, 2007).

[19] Phishing identification by learning on features of email received

Plusieurs autres auteurs vont proposer des améliorations incrémentales à l'approche d'apprentissage par machine appliquée au filtrage des pourriels. C'est notamment le cas de Hong et al. et de Trinius et al. (Rieck, Trinius, Willems, & Holz, 2011; Hong, 2012). Dans un autre article, He et al. proposent une approche heuristique pour déterminer si une page web est légitime (He et al., 2011). Cette approche est très répandue et exploitée par plusieurs autres auteurs dans leurs recherches (Y. Zhang, Hong, & Cranor, 2007; Rieck et al., 2011; Nguyen, To, Nguyen, & Nguyen, 2013). En fait, elle est une combinaison de la méthode CANTINA[20], de la méthode d'anomalie et de la méthode PILFER à laquelle on a apporté des modifications (Xiang, Hong, Rose, & Cranor, 2011). L'idée est de pouvoir détecter et différencier un site web légitime d'un site d'hameçonnage.

Plusieurs autres auteurs suggèrent que la signature numérique intégrée au courrier électronique soit utilisée comme contremesure au problème d'hameçonnage par pourriel. Parmi ces auteurs, il y a Gao et al., Garfinkel et al. et Jagatic et al.. Cette approche a le mérite d'utiliser un chiffrement de clé asymétrique (RSA[21]) et permet de distinguer clairement l'identité de l'expéditeur (Garfinkel & Cranor, 2005; Jagatic et al., 2007; Gao, Hu, Huang, Wang, & Chen, 2011).

L'article d'Adida et al. (2005) apporte une série de modifications à la signature électronique. Il propose une méthode pour mettre en œuvre une infrastructure légère de clés publiques (PKI) pour l'authentification par courrier électronique et un schéma de signature numérique spécifique à l'identité afin de rendre les courriels plus fiables. Ces améliorations sont très utilisées comme le montrent les articles de S. Kim et al. 2013 et 2015 (Adida, Hohenberger, & Rivest, 2005; S.-H. Kim, Choi, Jin, & Lee, 2013; S. Kim, Kang, & Kim, 2015).

La littérature est très vaste sur le sujet et plusieurs versions et améliorations des filtres de base que nous venons de présenter se trouvent dans l'article de Purkait et al. (Purkait, 2012). Le document discute, entre autre, de l'efficacité des listes noires du système de noms de domaine (DNSBL) et met en évidence un certain nombre de problèmes liés aux filtres, notamment, le taux de faux positifs dans les DNSBLs. Aussi, le document présente des solutions pour empêcher les courriels indésirables basés sur le filtrage bayésien. En effet, les filtres bayésiens établissent une corrélation

---

[20] Carnegie Mellon Anti-phishing and Network Analysis Tool

[21] L'acronyme RSA représente les initiales de ses trois inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman.

entre la présence de certains objets (ex. des mots, parfois des symboles, etc.) dans un message et leur apparition dans le courriel pour calculer la probabilité que ce courriel soit un hameçon. L'approche Bayésienne remonte à l'article de M. Sahami et al. (Sahami, Dumais, Heckerman, & Horvitz, 1998). Ces auteurs ramènent le problème dans le cadre de la théorie de la décision. Ils utilisent les méthodes d'apprentissage probabilistes en conjonction avec une notion de coût différentiel de mauvaise classification pour produire des filtres particulièrement adaptés aux nuances de l'hameçonnage (Sahami et al., 1998). Résultat, les filtres bayésiens sont parmi les plus précis.

Dans une autre étude, Lastdrager et al. présentent trois mécanismes d'authentification de l'expéditeur de courriel basés sur le DNS[22]: il y a la stratégie d'expéditeur (SPF), le mail identifié par les clés de domaine (DKIM) et l'identité de l'expéditeur (SIDF) (Lastdrager, 2014). Les auteurs soulignent les limites de ces mécanismes avant d'identifier les risques et de formuler les recommandations pour les travaux futurs.

2.4.2.2 Limites des filtres anti-hameçonnage

La première limite des filtres anti-hameçonnage vient du fait qu'un mauvais réglage des critères de rejet peut conduire à un taux de faux positifs élevé (courriels légitimes classés à tort comme hameçon) ou de faux négatifs (courriels hameçonnés non détectés) (Aublet-Cuvelier & da Cruz, 2011). Ces taux d'erreurs seraient de nature à miner la confiance des utilisateurs sur l'utilisation de ces filtres (Purkait, 2012). Aussi, les filtres sont par nature une réaction à une menace, ils n'empêchent pas «l'hameçonneur» d'envoyer des pourriels. Quant à la signature électronique, son inconvénient majeur réside dans les coûts d'implémentation et de formation.

2.4.2.3 Gestion des barres d'outils et des mots de passe

Pour cette catégorie de contremesures, C. Huang et al. font remarquer que plus de 70% des activités d'hameçonnage sont conçues pour voler les noms de comptes et les mots de passe des utilisateurs (C.-Y. Huang, Ma, & Chen, 2011). Les statistiques tirées des rapports 2016 et 2017 de l'APWG montrent que le nombre de sites web, conçus pour voler les mots de passe des utilisateurs, détectés

[22] Système de noms de domaine

est passé de 393K en 2014 à 1,22M en 2016, soit une augmentation de 310%. Quant au nombre de domaines où résident ces sites, ils ont augmenté de 23% par rapport à 2015 (APWG, 2016). Par conséquent, il est très important de prendre des mesures accrues de protection. Cette protection doit se faire aussi bien au niveau client qu'au niveau serveur. Au niveau client, le protocole HTTP de transfert hypertexte est très vulnérable aux attaques car les mots de passe circulent en clair sur Internet contrairement, par exemple, à la version sécurisée du même protocole (HTTPS) qui indique que la connexion entre le navigateur et le site web est cryptée afin d'empêcher toute tentative d'interception de données (Deuss, 2016).

Relativement à la gestion des mots de passe, plusieurs utilisateurs évitent de gérer de longues listes de mots de passe différents et privilégient un seul et même mot de passe pour plusieurs comptes. Le risque avec le mot de passe unique est qu'un attaquant peut voler ce mot de passe à partir des serveurs, même les plus sécurisés. Certains documents consultés proposent un protocole anti-hameçonnage à authentification unique. Ce protocole permet d'utiliser de manière sécurisée un mot de passe unique sur plusieurs serveurs, tout en évitant les attaques hameçonnées (Gouda, Liu, Leung, & Alam, 2007; Acar, Belenkiy, & Küpçü, 2013). Si le protocole sauve du temps grâce à une seule procédure d'authentification, son désavantage majeur vient du fait que lorsque le mot de passe unique est découvert, ce sont plusieurs comptes qui sont accessibles par les attaquants. Des outils basés sur le navigateur, côté client, ont été proposés afin de pallier cette vulnérabilité. Par exemple, Hard et al. ont enregistré un brevet d'invention sur la gestion des identités. Le gestionnaire qu'il propose est compatible avec toutes les applications Internet (Hardt & Grennan, 2008). Son principal atout, gérer en toute sécurité et simplicité les identifiants de sorte à ne retenir qu'un seul mot de passe.

Dans un autre article, Muchang et al. proposent une barre latérale du navigateur. Cette barre détecte les attaques par hameçonnage et suggère une alternative au choix de l'utilisateur. Les auteurs font remarquer, toutefois, qu'il est possible que le portefeuille web soit falsifié. Aussi, ils soulignent le fait qu'il y a un facteur purement humain. Les avertissements de sécurité donnés par ces barres d'outils sont interprétés par les internautes et certains n'y portent pas l'attention qu'il faut (Muchang, Trushchenkova, Somaiya, Jabbara, & Badley, 2015). Plusieurs variantes et extensions des barres d'outils des navigateurs ont été publiées au fil des ans. Nous ne les présenterons pas toutes ici, mais on peut noter AntiPhish et TrusBar.

L'AntiPhish est une extension du navigateur Mozilla de Firefox. Il protège les utilisateurs contre les attaques d'hameçonnage sur des sites. Pour ce faire, il suit les informations sensibles de l'utilisateur et génère des avertissements chaque fois que celui-ci tente de révéler ces informations sur un site web suspect.

TrusBar est une extension de navigateur pour sécuriser les sites protégés (SSL). TrustBar identifie les sites protégés par leur nom ou logo et par l'autorité de certification (CA) qui a identifié le site.

Dans deux autres études, les auteurs proposent une nouvelle technique qui utilise des fonctions de hachage cryptographique renforcée pour calculer les mots de passe sécurisés pour plusieurs comptes. La solution oblige l'utilisateur à mémoriser un mot de passe principal court. Ce mécanisme fonctionne entièrement du côté du client, mais du côté serveur aucun changement n'est requis (Halderman, Waters, & Felten, 2005; Wang & Qin, 2010). Jammalamadaka et al. utilisent cette nouvelle technique pour développer le système Pvault. Ce système utilise une fonction de remplissage manuel des mots de passe et autres informations sur des formulaires web. Ce qui peut empêcher le vol par hameçonnage. Cependant, un tel système a des limites. Par exemple, le système exige l'installation du logiciel client Pvault dans tous les ordinateurs distants qui accèdent au web. Aussi, toutes les entrées du système Pvault sont protégées par un mot de passe principal. Si ce dernier est compromis, toutes les entrées Pvault seront connues par l'adversaire. Il est par conséquent très important que les utilisateurs choisissent un mot de passe principal fort (Jammalamadaka, Mehrotra, & Venkatasubramanian, 2005). Un autre auteur exploite les mêmes concepts pour proposer une nouvelle technique appelée « Un cadre anti-phishing amélioré basé sur la cryptographie visuelle ». Dans son article, il présente une implémentation de l'authentification basée sur l'image et utilisant Visual Cryptography. Son approche utilise la cryptographie visuelle pour préserver la confidentialité de l'image en la décomposant en deux parties. Le serveur de confiance stocke des clés uniques nécessaires au décryptage du partage. L'image originale est obtenue à la fin uniquement lorsque l'utilisateur et le serveur sous test sont enregistrés auprès du serveur de confiance. En utilisant cette méthode, l'utilisateur peut déterminer si le site est sécurisé ou malicieux pour sa transaction (Palande, Jadhav, Malwade, & Baj, 2014). L'idée étant de faciliter la reconnaissance visuelle des sites contrefaits des sites légitimes.

Un nouveau concept est apparu il y a quelques années. Il s'agit du coffre-fort de données de confiance. Xiaolei et al. sont les premiers à concevoir et implanter un premier système - Droid

Vault – basé sur ce concept dans une plate-forme Android. Droid Vault établit un canal sécurisé entre les propriétaires de données et les utilisateurs de données tout en permettant aux propriétaires de données d'imposer un contrôle fort sur les données sensibles avec une base de calcul de confiance minimale (TCB). Un prototype Droid Vault est conçu grâce à la nouvelle utilisation des fonctionnalités de sécurité matérielle des processeurs ARM, à savoir, Trust Zone (Li et al., 2014).

D'autres extensions des navigateurs sont apparues sur le marché ces dernières années. On les retrouve sur Internet sous forme de plug in. A titre d'exemple, PwHash applique une fonction de hachage cryptographique à une combinaison du mot de passe en texte clair saisi par l'utilisateur, des données associées au site web qu'il veut accéder et une clé privée stockée sur le poste client. Ainsi, le vol d'un mot de passe d'un site donné ne fonctionnera pas sur un autre site.

Un autre exemple est celui du plug-in de navigateur appelé SpoofGuard. Ce plug-in surveille l'activité Internet d'un utilisateur, calcule un indice de contrefaçon et avertit l'utilisateur si cet indice dépasse un seuil qu'il se serait fixé au préalable. La solution utilise une combinaison d'évaluation de la page web sans état (vérification d'URL, vérification d'image, vérification de lien, vérification de mot de passe), d'évaluation de la page officielle (vérification de domaine, page de référence, association de domaine d'image) et de l'examen des données sortantes pour calculer un indice de contrefaçon. Lorsque l'on saisit un nom d'utilisateur et un mot de passe sur un site malicieux contenant une combinaison d'URL suspecte, de nom de domaine trompeur, d'images d'un site honnête, d'un nom d'utilisateur et d'un mot de passe précédemment utilisés sur un site honnête, il détecte une anomalie et avertit l'utilisateur par une fenêtre contextuelle. Toutefois, la solution proposée semble produire un taux de fausses alarmes très élevé en raison de l'utilisation du même mot de passe dans plusieurs sites différents ou lorsqu'on visite un site pour la première fois. Or, on sait qu'un utilisateur qui reçoit un nombre élevé de fausses alarmes peut s'y habituer et ne plus leur accorder l'attention qu'il faut (Mohammad, Thabtah, & McCluskey, 2012).

Enfin, selon Feng et al., la solution naïve d'empêcher le vol des mots de passe est d'éviter tout simplement d'utiliser les mots de passe. Les auteurs proposent un service d'authentification qui élimine le besoin de mots de passe utilisateur prédéfinis. Ils montrent que la solution proposée peut

être intégrée de manière transparente au service OpenID[23] afin que les sites web supportant OpenID en bénéficient directement. Cette solution peut être déployée de façon incrémentale et elle ne nécessite ni de plugin, ni de périphériques externes du côté client. Les auteurs croient que le nombre d'attaques d'hameçonnage pourrait être considérablement réduit si les utilisateurs n'étaient pas tenus de fournir leurs propres mots de passe lors de l'accès aux pages web (Feng, Tseng, Pan, Cheng, & Chen, 2011). Toutefois, cette solution soulève la question suivante: Est-il possible d'authentifier un utilisateur sans un mot de passe prédéfini?

2.4.2.4 Limites des barres de gestion des navigateurs et des mots de passe

La panoplie des barres d'outils sur Internet, la diversité des outils de gestion des mots de passe et l'absence de standard des navigateurs est de nature à créer une confusion chez les utilisateurs. Afin de pallier le problème de la variété de barres d'outils, certaines organisations ont mis en place des barres d'outils pour leur navigateur afin d'identifier les activités malicieuses. Mais là encore, l'utilisation que les employés en font et les comportements de ces employés lorsqu'ils utilisent ces navigateurs varient d'une personne à l'autre et ne garantissent pas l'efficacité attendue. Enfin, il y a les faux positifs. Ils peuvent dissuader les utilisateurs d'utiliser ces outils.

2.4.2.5 Listes de restrictions

L'hameçonnage étant une attaque web croissante à la fois en matière de sophistication, du volume et des techniques, les listes noires sont utilisées pour résister à ce type d'attaque (Sharifi & Siadati, 2008). Le principe est le suivant : le navigateur vérifie l'URL (Uniform Resource Locator) de la page web que l'on veut accéder dans une liste d'URL de sites d'hameçonnage connus. Si le site s'y trouve, le navigateur bloque l'accès et/ou génère un message d'avertissement indiquant le danger de ce site. Les listes noires sont construites en utilisant des techniques, les rapports manuels, l'analyse des liens, les pots de miel et les robots web, combinés à des heuristiques d'analyse de site (J. Ma, Saul, Savage, & Voelker, 2009; L. Ma, Ofoghi, Watters, & Brown, 2009; Luo, Zhang, Burd, & Seazzu, 2013). Cependant, ces listes noires ont deux problèmes majeurs. D'abord, elles

[23] C'est un système d'authentification décentralisé qui permet de s'authentifier sur plusieurs sites en utilisant le même identifiant (exemple Eduroam)

représentent une réponse réactive et non préventive au problème d'hameçonnage. Ensuite, leurs mises à jour ne sont pas automatiques.

Pour résoudre le second problème, l'article de Sharifi et al. propose une nouvelle technique et une architecture pour un générateur de listes noires des sites d'hameçonnage. Lorsqu'une page est reconnue comme appartenant à une entreprise donnée, le nom de l'entreprise est recherché à l'aide d'un moteur de recherche. Le domaine de la page est ensuite comparé au domaine de chacun des dix résultats recherchés de Google. Si un domaine correspondant est trouvé, la page est considérée comme une page légitime, sinon elle est considérée illégitime. L'évaluation préliminaire de cette technique a montré une précision de 91% dans la détection de pages légitimes et de 100% dans la détection de sites d'hameçonnage (Sharifi & Siadati, 2008). Quant au problème d'anticipation dans la mise à jour, Prakash et al. proposent PhishNet, une application qui prédit de nouvelles URL malveillantes à partir d'entrées de listes noires existantes. Au cours de l'évaluation de PhishNet avec des flux de listes noires en temps réel, les auteurs ont remarqué que l'approche proposée souffrait peu de faux positifs et était remarquablement efficace pour signaler de nouvelles URL qui ne faisaient pas partie des listes noires originales (Prakash, Kumar, Kompella, & Gupta, 2010). Dans une autre étude, Obied et al. développe une méthode basée sur les procurations pour empêcher l'accès de manière dynamique à des sites en tenant compte des cotes de sécurité établies par SiteAdvisor de McAfee (Obied & Alhajj, 2009).

Une autre approche de concevoir les systèmes de détection d'hameçonnage reposent principalement sur l'analyse des comportements des victimes. Deux articles permettent d'illustrer ce concept. Dans l'article de Dong et al, les auteurs proposent de construire une liste blanche des sites web que l'utilisateur a visités plus de trois fois. Le système envoie un signal d'avertissement à l'utilisateur si celui-ci souhaite visiter un site web qui n'est pas dans la liste blanche. De tels comportements d'utilisateur ne peuvent pas être manipulés librement par des attaquants. La détection basée sur ces données peut, non seulement atteindre une haute précision, mais aussi résister aux changements de méthodes de déception (Dong, Clark, & Jacob, 2008; Purkait, 2012).

L'analyse du comportement fait l'objet des travaux de Kovard et al. Ces auteurs présentent un système de détection de fraude pour la banque en ligne. Ce système est basée sur l'identification efficace des dispositifs utilisés pour accéder aux comptes et l'évaluation de la probabilité d'être une

fraude. Pour ce faire, le système effectue le suivi du nombre de comptes différents auxquels ont accès chaque périphérique (Kovach & Ruggiero, 2011).

Mais la même approche peut avoir des résultats limités si l'utilisateur ne respecte pas l'alerte donnée par la liste blanche. Comme l'ont expliqué Furnell et al., la plupart des utilisateurs ne savent pas ce qu'ils devraient faire lorsqu'une alarme de sécurité est lancée par le système (Furnell, Tsaganidi, & Phippen, 2008).

2.4.2.6 Limites des listes de restrictions

L'un des problèmes majeurs avec les listes noires est la mise à jour en temps réel des sites malicieux. Le problème est d'autant plus difficile que l'âge moyen de tout site d'hameçonnage varie de quelques heures à quelques jours seulement (Purkait, 2012). Les listes noires doivent donc être mises à jour en temps réel. Ce qui n'est pas toujours le cas.

En ce qui concerne les listes blanches, le problème est de deux ordres : l'utilisateur peut ne pas respecter les messages d'alerte que lui renvoie le système, auquel cas, il peut se retrouver en train de visiter les sites malicieux, ou alors, lorsqu'il change d'ordinateur et que sa liste blanche ne se synchronise avec une base de données centralisée, qu'il soit obligé de reconstruire une nouvelle liste blanche.

2.4.2.7 Détecteurs de sites d'hameçonnage

Il n'est pas aisé de différencier visuellement les sites d'hameçonnage, tant les technologies que les pirates utilisent sont de plus en plus sophistiquées. Les ressemblances entre sites contrefaits et sites légitimes sont telles qu'il est difficile pour quiconque qui n'est pas outillé de les détecter. Les premières méthodes de détection de sites contrefaits se sont inspirées de la technique basée sur le «Human Interactive Proofs –HIP-». C'est une technique qui permet à un humain de distinguer un ordinateur d'un autre. Dans une de leurs publications, Dhamija et al. exploitent cinq propriétés d'un HIP idéal pour détecter les attaques par hameçonnage. En utilisant ces propriétés, ils évaluent les systèmes anti-hameçonnage existants et proposent une nouvelle approche appelée Dynamic Security Skins (DSS). Ils montrent que cette approche répond aux critères HIP. Leur objectif est de permettre à un serveur distant de prouver son identité d'une manière qui soit facile pour un utilisateur humain de vérifier et difficile pour un attaquant de falsifier (Dhamija & Tygar, 2005). Toutefois, cette méthode a des limites : les utilisateurs ne s'interrogent généralement pas sur cet

indicateur avant d'entrer leurs mots de passe car l'approche DSS n'est pas dans le chemin critique du flux de travail de l'utilisateur (Wu, Miller, & Garfinkel, 2006).

Dans un article publié par Aburrous et al., une nouvelle approche pour surmonter la complexité de la détection est présentée. Les auteurs ont mis en place six algorithmes de classification différents et des techniques pour extraire les critères de données de formation d'hameçonnage afin de classer leur légitimité. Une étude de cas a été faite et les résultats expérimentaux ont démontré la faisabilité de telles techniques de classification associative et leur meilleure performance par rapport à d'autres algorithmes de classification traditionnelle (Aburrous, Hossain, Dahal, & Thabtah, 2010). Mais cette approche ne règle pas le problème des attaques de type «man-in-the-middle». Ce type d'attaques constitue une grave menace pour les applications de commerce électronique basées sur SSL/TLS, telles que les services bancaires par Internet. Dans un livre publié par Lunde et al., les auteurs soutiennent que la plupart des mécanismes d'authentification des utilisateurs déployés ne fournissent pas de protection contre ce type d'attaque, même lorsqu'ils s'exécutent sur SSL/TLS. Ils présentent la notion d'authentification utilisateur par session SSL/TLS et les différentes possibilités de mise en œuvre. Son implémentation de base emploie des jetons d'authentification impersonnels. Ensuite, ils discutent des possibilités de mise en œuvre de l'authentification des utilisateurs SSL/TLS dans les logiciels (Lunde, Franklin, Lulich, & Pierson, 2007).

D'autres travaux de recherche ont exploré les caractéristiques des codes sources des pages web qui distinguent les sites d'hameçonnage des sites légitimes afin de détecter les attaques. Alkhozae et al. publient dans un article un exemple d'utilisation de cette technique. Ils extraient certaines caractéristiques d'hameçonnage des normes W3C[24] pour évaluer la sécurité des sites et vérifier chaque caractère dans le code source de la page web. Lorsque la page est trouvée, on diminue le poids initial de sécurité. Enfin, ils calculent le pourcentage de sécurité en fonction du poids final, le pourcentage élevé indique un site web sécurisé et l'inverse indique que le site est susceptible d'être un site malveillant (Alkhozae & Batarfi, 2011).

Dans un autre article, Saklikar introduit le concept de CAPTCHA graphique intégré à clé publique et leur utilisation comme mécanisme anti-hameçonnage. Le terme CAPTCHA en soi est emprunté. C'est une marque déposée par l'université Carnegie-Mellon. Il désigne une série de tests de Turing

[24] World Wide web Consortium

dont l'objectif est de différencier de façon automatisée un utilisateur humain d'un ordinateur. L'auteur adapte ce concept de sorte à ce que les CAPTCHA contiennent un objet d'image spécifique à l'utilisateur et un motif de canal sécurisé (par exemple, la clé publique du serveur web authentique), dans lequel l'objet et le motif d'image sont liés. En vertu d'un mécanisme de défi impliqué intégralement bidirectionnel et de cette association vérifiable entre l'objet image et le sous-modèle spécifique de la clé publique. Ils aident à détecter / résister aux attaques par hameçonnage automatisées ou assistées par l'homme (Saklikar & Saha, 2008). Leung dans son travail montre les limites de CAPTCHA dans la sécurisation des services bancaires en ligne avec une série de tests sur une implémentation CAPTCHA d'une banque locale. L'étude montre comment CAPTCHA peut être contourné. L'auteur propose un système de saisie CAPTCHA étendu pour décourager les «hameçonneurs» en utilisant la restriction de temps du mot de passe à usage unique (OTP[25]) (Leung, 2009).

Dans leur publication de 2011, Zhang et al ont proposé un nouveau système anti-phishing basé sur une analyse du contenu qui s'appuie sur la théorie bayésienne. Le cadre proposé comprend un classificateur de texte, un classificateur d'image et un algorithme de fusion. Sur la base du contenu textuel, le classificateur de texte est capable de classer une page web donnée dans des catégories correspondantes (légitime ou illégitime). Sur la base du contenu visuel, le classificateur d'image, qui repose sur la distance des moteurs terrestres (EMD), est capable de calculer efficacement la similitude visuelle entre la page web donnée et la page protégée. Le seuil d'appariement utilisé dans le classificateur de texte et dans celui d'image est estimé en utilisant un modèle probabiliste dérivé de la théorie bayésienne (H. Zhang, Liu, Chow, & Liu, 2011).

La compagnie Phishing Inc. a enregistré un brevet qui décrit les méthodes, les périphériques réseaux et les supports de stockage lisibles par machine pour détecter si un message est une attaque d'hameçonnage. Cette approche est basée sur les réponses collectives d'une ou plusieurs personnes qui ont reçu ce message. Les individus peuvent signaler le message comme une éventuelle attaque et/ou peuvent fournir un classement numérique indiquant la probabilité que le message soit une éventuelle attaque. Comme les réponses de différents individus peuvent avoir un degré de fiabilité différent, chaque réponse d'un individu peut être pondérée avec un niveau de fiabilité

[25] One-time password

correspondant de cette personne. Un niveau de confiance d'un individu peut indiquer un degré dans lequel la réponse de cet individu peut être confiée et/ou dépendante, et peut être déterminée par la façon dont cet individu a reconnu des attaques d'hameçonnage simulées (Higbee, Belani, & Greaux, 2016).

Un autre brevet, enregistrée par la compagnie Adi Labs Incorporated, porte sur un procédé hybride contrôlé par un processeur, un appareil et un support de stockage lisible par ordinateur pour identifier une page web illégitime. Le procédé consiste à capter les informations visuelles et structurelles globales d'une page web parcourue par un utilisateur puis, à les comparer avec les mêmes genres d'informations relatives aux sites légitimes ou sites d'hameçonnage qui ont été stockées préalablement dans une base de données. Ensuite, on calcule une mesure de similarité qui est comparée à un seuil prédéterminé. Cette mesure permet de dire si un site est légitime ou pas (Gupta, Tanbeer, & Mohandas, 2017).

2.4.2.8 Limites des détecteurs de sites d'hameçonnage

Les efforts de recherche ont été faits au fil des ans pour la détection des pages et sites web d'hameçonnage. Cependant, toutes les approches existantes que nous avons étudiées ont des limites, telles que la nécessité d'avoir des connaissances préalables sur l'authenticité des sites, sur la contrefaçon des sites et sur l'hameçonnage en général. Les outils de détection les plus efficaces sont des inventions, des brevets et ne sont pas accessibles à tous.

2.4.2.9 Authentification multiple

Le mot de passe est le moyen d'authentification le plus répandu pour se connecter à des sites web. Pour chaque site, un mot de passe est mémorisé et, pour chaque connexion, il est utilisé pour s'authentifier. Sa vulnérabilité vient du fait que certains utilisateurs utilisent le même mot de passe sur plusieurs sites et lorsque ce mot de passe est compromis alors ce sont plusieurs comptes qui sont compromis (X. Chen, Bose, Leung, & Guo, 2011). Afin de résoudre ce problème, les recherches ont proposé l'authentification à deux facteurs. Ce type d'authentification permet de garantir que l'utilisateur est la seule personne qui peut accéder à son compte même si son mot de passe est compromis. Ce système d'authentification fonctionne en deux temps. Dans un premier temps, l'utilisateur introduit son nom de compte et son mot de passe et, dans une seconde étape, le système lui demande une information dont il est le seul à la connaître. Par exemple, dans l'article

de Fang et al., le concept de jeton de génération de mot de passe (PGT) est utilisé pour la mise en œuvre de l'application SecureID de RSA. Le système fonctionne comme suit : une fois qu'un client fournit son nom d'utilisateur et son mot de passe original à la banque via Internet, un mot de passe unique est envoyé par SMS (Short Message Service) à son téléphone cellulaire. L'utilisateur récupère ensuite ce mot de passe de son mobile et l'utilise pour une nouvelle connexion (Fang & Zhan, 2010). Dans certains cas de figure, ce sont des questions de sécurité préalablement enregistrées avec des réponses qui sont posées afin de s'assurer que l'utilisateur du mot de passe est bien celui qu'il prétend être.

La compagnie N-Dimension Solutions Inc. a enregistré un brevet sur l'authentification à deux facteurs. Le système qu'elle propose implémente une routine d'authentification qui permet à la fois de s'authentifier sur un système (ex. VPN) et valider l'accès à d'autres systèmes sécurisés indépendamment (Austin, Wan, & Wright, 2013).

La biométrie est également une préoccupation de sécurité dans le processus d'authentification bancaire en ligne, où un utilisateur doit s'authentifier en effectuant des analyses d'iris ou d'empreintes digitales ou des confirmations vocales. L'infrastructure à clé publique (PKI) est appliquée à l'authentification en ligne. Le protocole de transfert hypertexte sécurisé (HTTPS) est largement adopté, non seulement pour l'authentification bancaire en ligne, mais aussi pour les achats en ligne et les authentifications de système de messagerie. Avec la mise en œuvre de HTTPS, un client peut être authentifié en fournissant son certificat numérique à la banque (Fang & Zhan, 2010).

Dans l'article de Hartung et al., le protocole d'authentification des transactions biométriques (BTAP) proposé repose sur la protection du schéma de données pour un modèle biométrique et sur un dispositif de transaction biométrique fiable. BTAP offre des transactions authentiques en fusionnant les informations pertinentes sur les transactions financières en ligne avec des informations biométriques sécurisées sur la personne physique de sorte qu'il soit prouvé à l'autre partie que la transaction telle qu'elle est reçue a été, en effet, initiée et confirmée par une personne physique identifiée (Hartung & Busch, 2010).

2.4.2.10 Limites de l'authentification multiple

Bien que son utilisation soit très repandue, l'authentification à deux facteurs pose un souci quand même car les codes à usage unique (OTP) sont souvent envoyés par SMS en texte clair sur le

téléphone cellulaire de l'utilisateur. Ce qui n'est pas très sécuritaire. En cas de perte ou de vol de téléphones cellulaires, le code OTP est connu. Les messages SMS peuvent également être interceptés et transmis à un autre numéro de téléphone, ce qui permettrait à un cybercriminel de recevoir le code OTP (Purkait, 2012).

2.4.2.11 Journalisation des sites hameçonnés

Nous avons présenté au paragraphe 2.4.2.7 intitulé détecteurs de sites d'hameçonnage une revue des approches pour reconnaître qu'un site est malicieux. Lorsque ces sites sont détectés, ils sont enregistrés dans des listes noires. Ensuite, avec des techniques de blocage de sites suspects qui ont été identifiés par rapport aux listes noires, on peut les mettre hors d'état de nuire. Toutefois, avec de telles techniques, on a de la difficulté à suivre les traces de ces sites car leur durée de vie varie de quelques heures à quelques jours seulement (Purkait, 2012). De plus, ces techniques s'appuient sur une analyse hors ligne. Elles ne sont pas assez robustes pour suivre le rythme d'apparition et de disparition des sites d'hameçonnage et ne donnent pas des messages de mise en garde aux utilisateurs. Pour remédier à ces limites, Giovannie Armano a développé un logiciel de prévention en temps réel de l'hameçonnage côté utilisateur qui utilise une technique de détection d'hameçonnage développée par Marchal et al.. Son logiciel extrait les informations de la page web visitée et détecte s'il s'agit d'un hameçon, le cas échéant il avertit l'utilisateur. Il est également capable de détecter le site que «l'hameçonneur» tente d'imiter et de proposer une redirection vers le domaine légitime (Armano, 2016). Toutefois, le site d'hameçonnage reste en activité. L'un des moyens pour le mettre hors d'état de nuire est connu sous le nom de «take-down». Il s'agit par exemple, pour les banques et d'autres organisations, de demander la collaboration des hébergeurs de sites web afin qu'ils suppriment les sites d'hameçonnage dès qu'ils sont détectés (Tyler Moore & Clayton, 2007). Cette collaboration nécessite, dans certains cas, les efforts des utilisateurs finaux. En effet, des sites web et des outils ont été développés pour solliciter la collaboration des utilisateurs finaux. Par exemple, PhishTank est un site de collaboration mis en ligne en 2006 par David Ulevitch pour inviter les utilisateurs à soumettre les informations sur les sites qu'ils considèrent comme étant des sites suspects et ainsi permettre à d'autres utilisateurs de voter (OpenDNS, 2016). L'inconvénient d'une telle approche est relevé par Moore et Clayton qui ont analysé les données reçues des auteurs de PhishTank et ont conclu que tout mécanisme de décision fondé sur le public comme ce que font les auteurs de PhishTank demeure susceptible de

manipulation de vote. Ce qui pourrait compromettre sa crédibilité (Tyler Moore & Clayton, 2008). Ces auteurs concluent également que la suppression pure et simple des sites d'hameçonnage dès qu'ils sont découverts restent la solution aux attaques par hameçonnage. Cependant, la lenteur avec laquelle cette suppression se fait ne garantit pas l'efficacité de l'approche car les attaquants ont le temps et les outils nécessaires pour créer de nouveaux sites.

Dans un rapport publié en 2005, Aaron Emigh propose une analyse des fichiers de journalisation afin de détecter les leurres d'hameçonnage. Selon cet auteur, ce mécanisme peut considérablement améliorer la réactivité dont on a besoin pour supprimer en ligne les sites d'hameçonnage. En effet, si les journaux sont surveillés en temps réel, des temps de réponse très rapides pourraient être atteints (Emigh, 2005). L'auteur publie en 2014 un brevet d'invention qui analyse les liens entre diverses destinations, différents adresses et paramètres compris dans le courrier électronique et en fonction des vérifications dans une liste noire, on peut autoriser ou pas la navigation sur un site.

2.4.2.12 Limites de la journalisation

Les sites d'hameçonnage sont souvent hébergés gratuitement et accessibles de partout. Les attaquants peuvent se trouver dans un continent et faire héberger leur site dans un autre. De plus, les serveurs qui hébergent ces sites d'hameçonnage utilisent des flux très rapides leur permettant de résoudre un très grand nombre d'adresses IP avec des baux de très courtes durées (McGrath, Kalafut, & Gupta, 2009). Ce qui donne aux attaquants une grande capacité de réaction en cas de détection. Cela pose le problème de limitation des pouvoirs juridiques lorsque vient le moment de collaborer pour mettre à jour voire supprimer rapidement les listes de sites malveillants.

Aussi, la journalisation est une réaction et non de la prévention. «L'hameçonneur» agit et en réponse on met à jour les enregistrements dans le journal et, lorsque possible, on fait supprimer le site. Ce qui explique que «l'hameçonneur» est toujours en avance et aucune de ces dispositions ne permet d'anticiper son action. Enfin, la journalisation des sites hameçonnés implique un facteur purement humain.

2.4.3 Contremesures éducatives et de sensibilisation

La sensibilisation des utilisateurs à ce phénomène reste l'un des meilleurs moyens de lutte contre toutes les formes d'hameçonnage (Trudel et al., 2007). Depuis plusieurs années, des campagnes de sensibilisation sont menées aussi bien auprès des utilisateurs que dans des organisations (publiques

et privées). Au Canada, le mois de mars a même été déclaré comme étant le mois de la sensibilisation à la fraude. Le Centre antifraude du Canada (CAFC) recommande aux consommateurs et aux entreprises de se méfier des diverses tactiques de fraude à l'identité utilisées par les hackers (CAFC, 2017). Du côté des banques et institutions émettrices de cartes de crédit, l'information sur la fraude est disponible sur leurs sites, dans des brochures destinées aux utilisateurs, et des conseils pratiques sur la façon de se protéger sont également offerts. Essentiellement, il s'agit d'apprendre aux utilisateurs à reconnaître :

- les signes d'une tentative d'hameçonnage (les faux noms de domaine, les hyperliens truqués, les différents stratagèmes, etc.);
- les sites web sécurités valides, etc.

Dodge et al. intègrent un exercice de formation et de sensibilisation dans une application informatique pour évaluer la propension des utilisateurs à répondre aux attaques par hameçonnage lors d'un test non annoncé. L'article décrit les considérations dans l'établissement et le processus utilisé pour créer et mettre en œuvre une évaluation d'un aspect du programme d'éducation sur l'assurance des informations utilisateur (Dodge, Carver, & Ferguson, 2007). Dans un autre travail similaire, Jansson et al. ont mené en Afrique du Sud une simulation d'attaques par hameçonnage avec une formation intégrée et confirme que celle-ci a contribué à cultiver la résistance des utilisateurs face aux «attaques par hameçonnage» (Jansson & von Solms, 2013).

Une autre stratégie de sensibilisation contre l'hameçonnage exploite à la fois l'efficacité des technologies de l'information et les atouts de la communication. Cette stratégie consiste à utiliser davantage des interfaces interactives pour sensibiliser les utilisateurs sur les risques auxquels les cyber-menaces les exposent et sur l'importance de se protéger. Plusieurs innovations ont été faites dans ce sens. On a intégré aux interfaces d'antivirus, des modules d'alertes et d'avertissements qui mettent en garde l'utilisateur contre les sites web suspects. Le problème avec ces avertissements de sécurité est que certains utilisateurs les ignorent. Un comportement qui augmente les chances de se faire prendre par un hameçon. D'où l'importance de sensibiliser constamment les utilisateurs sur tous ces enjeux.

Une étude menée par Kumaraguru et al. en 2010 avait conclu que ce genre sensibilisation était très utile pour aider les gens à identifier les faux sites web (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). D'autres outils ont été développés. Parmi ces outils, il y a les micro-jeux conçus pour

enseigner aux utilisateurs à reconnaître et éviter les cyber-menaces. Sheng et al. ont développé un micro-jeu appelé Anti-Phishing Phil. Ce jeu enseigne comment reconnaître sur les barres d'adresse des navigateurs les noms de domaine et des pages d'hameçonnage, puis teste les connaissances des utilisateurs sur ce qu'ils ont appris. Une évaluation d'Anti-Phishing Phil. sur plus de 4500 participants a conclu que son utilisation a permis d'améliorer la capacité des novices à identifier l'hameçonnage de 61% tout en réduisant considérablement les faux positifs.

La dernière stratégie de sensibilisation est ce qu'on appelle la formation intégrée. Elle consiste à former l'utilisateur dans son contexte naturel d'utilisation d'Internet où il se fait habituellement attaquer. Kumaraguru et al. ont mis au point un système de formation intégrée appelé PhishGuru. Ce système a été testé auprès de 500 participants. Les résultats démontrent qu'il y a une réduction de 45% des cas d'hameçonnage entre le début et la fin de la formation.

2.4.3.1 Limites des programmes formation et de sensibilisation

La première difficulté est que les formations contre l'hameçonnage ne sont pas renouvelées au rythme de parution des menaces. Or, pour faire face à une menace qui change à un rythme effréné, il faut des programmes de formation et de sensibilisation qui s'ajustent à ces changements. Il faut que les interfaces et autres outils de communication qui viennent en support à cette formation soient mis à jour régulièrement. Tout ceci entraine des coûts que les utilisateurs et les organisations qui les emploient ne sont pas toujours prêts à défrayer. Plus important encore, les programmes de formation en place ne sont pas toujours adaptés à l'auditoire et à la gravité du problème. Des études antérieures sur la formation ont montré que ces formations testent les utilisateurs sur des scénarios prédéfinis où les sites d'hameçonnage sont connus d'avance. Il serait intéressant de voir comment le même utilisateur réagit à une attaque par hameçonnage en temps normal sans être informé d'avance (Purkait, 2012).

2.4.4 Contremesures administratives et opérationnelles

Cette catégorie de contremesures relève purement de la stratégie de défense et peut impliquer l'un et/ou l'autre des types de contremesures que nous avons décrit plus haut (Zhuang, Bier, & Alagoz, 2010). Il s'agit de mettre en place une politique, des contremesures et des procédures de sécurité en fonction de la menace. Par exemple, dans une entreprise, certaines de ces contremesures peuvent prendre la forme de bonnes pratiques de gestions des correctifs, des règles de filtrage, des

programmes de formation, des définitions des actions à entreprendre par différents responsables, etc.

Dans l'article de Zhuang et al., les auteurs appliquent la théorie des jeux pour modéliser les stratégies de l'attaquant et du défenseur avec des informations incomplètes. L'idée étant de deviner le secret et/ou la tromperie du défenseur (Zhuang et al., 2010). En fait, le défenseur et l'attaquant rentrent dans une espèce de jeu séquentiel où chacun déploie des stratégies selon ses gains ou pertes (Shan & Zhuang, 2013), où le défenseur peut mettre à la disposition des attaquants une information imparfaite sur ses stratégies de défense. C'est dans cette dynamique que le défenseur déploie et reconfigure ses contremesures constamment afin de contrer la stratégie de l'attaquant.

Dans un autre article, Roy et al. présentent une nouvelle approche pour fournir uniquement des informations limitées et nécessaires au transfert de fonds lors des achats en ligne. Ce qui permet de sauvegarder les données des clients et d'accroître leur confiance tout en prévenant le vol d'identité. La méthode combine la stéganographie et la cryptographie visuelle. La stéganographie est l'art de dissimuler un message dans un autre afin que le message caché soit indiscernable. Le concept clé derrière la stéganographie est que le message à transmettre ne soit pas détectable à l'œil nu (Roy & Venkateswaran, 2014).

D'autres travaux de recherche ont utilisé cette méthode bien avant Roy et al. Parmi ces travaux, il y a ceux de Premkumar et al. Ils proposent une technique de codage du mot de passe d'un client par l'approche de Steganographie améliorée. En effet, la plupart des techniques steganographiques utilisent trois ou quatre pixels adjacents autour du pixel que l'on veut cacher alors que la technique proposée dans cet article est capable d'utiliser huit pixels adjacents de sorte que la valeur d'imperceptibilité augmente. Ensuite, le décodage est utilisé pour récupérer le mot de passe caché (Premkumar & Narayanan, 2012).

D'autres mécanismes de sécurisation des transactions existent et sont complémentaires à la technique de chiffrement de transaction que nous venons d'exposer. Parmi ces mécanismes, il y a l'utilisation des témoins. Un témoin est un fichier contenant des éléments d'information que le site web de la banque crée automatiquement lorsqu'un client le visite. Par exemple, lorsqu'un client se connecte à un service bancaire en ligne, le serveur dudit service capture les informations liées à sa session active et, pendant toute la durée d'utilisation du service en ligne, il effectue les vérifications nécessaires pour s'assurer que la banque fait affaire avec le bon client. Cet outil comble la lacune

de la journalisation en ce sens que les fichiers journaux contiennent des données qui manquent de précision contrairement aux fichiers témoins qui permettent d'attribuer un numéro unique à chaque visiteur afin de le suivre et, peu importe l'adresse IP qu'il utilise. Cette méthode a été utilisée par Chassigneux en 2003 pour construire un outil d'analyse basé sur Internet qui suit, en temps réel, le flux de trafic via un site web. Pour chaque page web demandée par un visiteur, l'état du navigateur du visiteur est enregistré et les données relatives au chemin parcouru par le visiteur sont collectées et analysées. L'état du chemin du navigateur du visiteur est maintenu dans un cookie afin de permettre l'analyse du trafic entre le serveur du site web, le navigateur du visiteur et chaque page consultée. Les données dans le cookie peuvent suivre le navigateur via des serveurs de fichiers indépendants, peu importe la façon dont les pages du site web sont distribuées en mémoire (Chassigneux, 2003).

Diverses autres approches ont été proposées afin de gagner la confiance des utilisateurs lors des transactions en ligne. L'article de Yildiz et al. propose une nouvelle solution qui combine l'identité biométrique avec les informations sur les transactions en ligne (Yildiz & Göktürk, 2010).

2.4.4.1 Limites de ces mesures administratives et opérationnelles

Dans leur article, Lao et al. soulignent que les problèmes de sécurité peuvent être résumés en deux catégories : les problèmes liés à la sécurité des systèmes et ceux inhérents à la sécurité de l'information (Lao & Wang, 2010). La sécurité des systèmes (ex. serveurs, applications, etc.) et particulièrement celle qui est mise en place par les banques est très fiable. En revanche, du côté client, c'est loin d'être le cas. Selon Nuha et al., la sécurité de l'information pose problème. Elle repose plus souvent sur la technologie et beaucoup moins sur la prise de conscience des enjeux de sécurité par les clients et les organisations. Résultat, l'utilisation des contremesures technologiques n'est pas optimale car l'utilisateur ne les exploitent pas en prenant suffisamment en compte les menaces (Nuha & Asadullah, 2013). Du côté de la banque la sensibilisation qui est faite sur les menaces ne suffit pas non plus. L'article de Delgado et al. conclut que, malgré le niveau élevé de protection des systèmes de sécurité de la banque en ligne, ces systèmes restent quelque part vulnérables à des attaques, et particulièrement aux attaques de l'homme du milieu (man-in-the-middle attack - MITM) (Delgado, Fuster-Sabater, & Sierra, 2008). Les attaques de l'homme du milieu visent à intercepter les communications entre deux parties (ex. la banque et le client), sans que ni l'une ni l'autre ne puisse se douter que le canal de communication est compromis (Hisamatsu,

Pishva, & Nishantha, 2010). Ce constat est confirmé dans le dernier rapport de Proofpoint où l'auteur y déclare que « nous sommes toujours les principaux maillons faibles de la cyber-sécurité » (Proofpoint, 2017).

2.5 Monétisation

Les références consultées sur les marchés noirs ont été regroupées en deux grandes catégories afin de respecter l'orientation de notre sujet de thèse. Nous avons regroupé dans la première catégorie toutes les références qui décrivent les marchés noirs, leurs acteurs, les biens et services qui s'y transigent et le modus operandi de ces marchés. Ensuite, dans une deuxième catégorie, nous avons regroupé les références qui analysent les activités de ces marchés avec les outils microéconomiques.

2.5.1 Le fonctionnement du marché noir

L'examen de la littérature sur le fonctionnement des marchés noirs a relevé un certain nombre d'éléments caractéristiques de ces marchés, notamment, les acteurs, les biens et services et le modus operandi (Tyler Moore, Clayton, & Anderson, 2009; Holt & Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011; Mell, 2012; Holt, 2013a, 2013b). En ce qui concerne les acteurs, l'ensemble des travaux consultés s'accordent sur quatre types d'acteurs principaux. Il y a au début du processus le fraudeur, c'est celui qui initie la fraude en achetant les renseignements bancaires au marché noir avec comme objectif de voler de l'argent. Et, à l'autre extrémité, on retrouve la victime. Entre les deux, il y a plusieurs métiers spécialisés que nous avons regroupés en deux sous-catégories : les vendeurs et les intermédiaires. Le vendeur, c'est celui qui échange et vend les renseignements dérobés à d'autres cybercriminels alors que l'intermédiaire effectue les transferts entre comptes bancaires ou par divers canaux -nationaux ou internationaux- de transfert d'argent, faisant ainsi office de passeur ou de blanchisseur de gains de la cybercriminalité (Panda, 2011).

Derrière chacun de ces principaux acteurs, on retrouve d'autres postes comme le développeur de malware, le hacker[26] et l'administrateur de forums qui contribuent à subtiliser les renseignements

[26] Ils recherchent des vulnérabilités et exploitent les failles de sécurité d'applications, systèmes et réseaux

relatifs aux comptes des victimes, à les mettre à la disposition du vendeur ou à réguler les transactions dans des forums. Tout comme derrière l'intermédiaire, on retrouve les mules[27], les blanchisseurs[28], les responsables des organisations criminelles et les entreprises de services. Ces «métiers» de l'activité de monétisation et leurs rôles respectifs sont très bien définis selon la typologie du FBI (Panda, 2011).

En ce qui a trait au mode opératoire, plusieurs travaux de recherche abordent la question (Tyler Moore et al., 2009; Shulman, 2010; Holt & Lampke, 2010; Motoyama et al., 2011; Sood, Bansal, & Enbody, 2013). Les auteurs s'accordent pour dire qu'il est assez complexe. Dans son article sur la cartographie économique de la cybercriminalité, Cárdenas explique que lorsque les hackers mettent la main sur des renseignements bancaires, ils ont peu d'alternatives. Soit ils recrutent les mules sur Internet pour monétiser ces renseignements, soit ils revendent les données brutes à d'autres cybercriminels, ou alors ils concluent des ententes avec des professionnels « Cash out » - c'est-à-dire, des criminels qui se spécialisent dans la fabrication des cartes bancaires et qui utilisent les personnes physiques pour retirer l'argent à partir du guichet ou qui se présentent carrément au comptoir des banques pour faire des retraits (Cárdenas, Radosavac, Grossklags, Chuang, & Hoofnagle, 2010). Ce dernier processus est plus risqué et par conséquent est très onéreux comme l'explique Sood dans son article sur l'état des lieux des marchés noirs (Sood et al., 2013). Les fraudeurs qui font affaire avec un intermédiaire versent à ce dernier généralement un pourcentage pouvant aller jusqu'à 40 voire même 60 pour cent du montant de la transaction. Tous ces services reposent sur la confiance que les acteurs des marchés noirs ont en ce système. Cette notion de confiance est abordée par Andrew Mell sous l'angle de la réputation. Il examine le système de réputation qui est utilisé dans ces marchés. Il relève que les forums clandestins attribuent en général à un vendeur un statut qu'on peut facilement observer dans le forum car une étiquette y est associée (Mell, 2012). Ainsi, un vendeur peut être qualifié de «vérifié[29], non vérifié, ou ripper[30]". Ces statuts constituent le socle de la confiance et assurent que les données vendues par des «vendeurs vérifiés» sont authentiques. En revanche, ces mécanismes constituent un talon d'Achille que les services de

---

[27] Ce sont les passeurs qui effectuent les transferts entre comptes bancaires

[28] Ils sont chargés du blanchiment des gains illicites via divers systèmes mondiaux de change et transfert d'argent

[29] Le vendeur «vérifié» est celui dont un échantillon des données a été testé par l'administrateur du forum qui en confirme l'authenticité.

[30] Le vendeur ripper est celui qui a perdu la confiance des clients et de l'administrateur du forum.

police exploitent en infiltrant les forums afin de bâtir leur réputation et nuire aussi bien aux vendeurs qu'aux acheteurs (Mell, 2012).

D'autres travaux conduits par Aston et al. Florênco et al. et Mell soulignent que le fraudeur agit, dans un marché noir, comme tout agent économique le ferait dans n'importe quel autre marché formel. C'est-à-dire qu'il cherche à maximiser son gain (Aston, McCombie, Reardon, & Watters, 2009; Florêncio & Herley, 2010; Mell, 2012). Ils font le parallèle entre les facteurs de production dans un marché formel et les facteurs de monétisation dans le marché noir. Pour ces auteurs, le profit du fraudeur est étroitement lié aux facteurs de monétisation. Motoyama et al. identifient deux de ces facteurs : la confiance entre les acteurs et la réputation des vendeurs (Herley & Florêncio, 2010; Motoyama et al., 2011). D'autres travaux menés par Florêncio et al, et Thomas et al. (Cymru, 2006; Florêncio & Herley, 2010) identifient le facteur de commissions payées à la mule pour faire monétiser un renseignement. Selon eux, il existe une offre insuffisante de mules pour disposer des comptes compromis. Quant au prix des renseignements, c'est un facteur qui varie énormément d'un forum à l'autre et même d'un vendeur à l'autre à l'intérieur du même forum. Ablon et al. (Lillian Ablon, Martin C. Libicki, & Golay, 2014) traitent du même sujet. Ils expliquent la variation du prix par l'âge du renseignement sur le marché. Par exemple, le prix des cartes de crédit nouvellement acquises est plus élevé immédiatement après que le vol des données ait eu lieu. Puis, le prix diminue avec le temps.

En ce qui concerne les obstacles inhérents au processus de monétisation, Herley explique qu'une des difficultés de monétisation est le caractère réversible des transactions bancaires –annulation possible- qui oblige le fraudeur à avoir recours au service de «mule» pour soutirer de l'argent du compte de sa victime (Herley, 2014).

2.5.2 Les modèles économiques de la criminalité

Le modèle d'avant-garde cité en économie du crime est, sans aucun doute, celui de Gary Becker (Becker, 1968, 1974). L'économiste fait l'hypothèse que le criminel, avant de commettre un crime, fait le calcul rationnel entre les gains espérés du crime, en tenant compte de la probabilité d'être arrêté, et le type, voire la gravité, de la sanction, comparé au gain du travail accompli en toute légalité. Son modèle montre que la décision optimale est celle qui minimise les pertes sociales. Il montre aussi que, pour maximiser le revenu social total, les sanctions optimales contre les criminels devraient prendre la forme d'amendes. Il fait valoir que les amendes sont une meilleure dissuasion

du crime que l'emprisonnement qui lui, coûte plus cher à la société. Une idée que reprend Cárdenas dans (Cárdenas et al., 2010). De son modèle, nous retenons deux idées principales : l'idée que le criminel évalue les coûts et bénéfices du crime avant de passer à l'acte et celle que cette évaluation prend en compte la valeur monétaire des sanctions y afférentes.

Le modèle de Kshetri (Kshetri, 2006) reprend ces idées dans sa formule de calcul du coût bénéfice d'un pirate. Il suggère des mécanismes de lutte contre la cybercriminalité. Le cadre qu'il propose décrit la façon dont les caractéristiques des cybercriminels, les organismes qui sont chargés d'appliquer la loi, et les victimes de la cybercriminalité façonnent le paysage de la cybercriminalité. Pour l'auteur, le manque de confiance aux organismes en charge d'appliquer la loi, la faiblesse des mécanismes de défense, le faible taux des plaintes sont les causes de l'augmentation de la confiance des cybercriminels et des liens de plus en plus forts que ces réseaux entretiennent avec le crime organisé. Toutefois, l'auteur introduit dans sa formule de calcul une composante représentant les avantages psychologiques et dont l'évaluation poserait problème. En effet, l'énergie psychologique et mentale nécessaire pour mener une activité cybercriminelle est intangible car elle résulte plus de la crainte des sanctions ou de la culpabilité (Kshetri, 2006). Cependant, l'article n'explique pas comment mesurer cette composante. Aussi, l'approche d'évaluation monétaire n'est pas explicitement formulée.

Les modèles ci-dessus ont en commun de prendre en compte deux éléments dans la prise de décision du fraudeur : les coûts de monétisation et la valeur monétaire des sanctions. L'examen de la littérature révèle que peu d'articles traitent simultanément de ces deux éléments, en revanche, plusieurs modèles et auteurs abordent séparément chacun de ces éléments.

Relativement à la valeur monétaire des sanctions et de leurs impacts dans la prise de décision du fraudeur, elle a été abordée par plusieurs auteurs, et notamment par Garry Becker, Mitchell Polinsky, Giovanni Mastrobuoni et Pierre Kopp (Becker, 1968, 1974; Kopp, 2003; Polinsky & Shavell, 2007; Mastrobuoni, 2011) pour ne citer que ceux-là. Mitchell Polinsky revisite la théorie de maximisation du bien-être social et l'application de la loi contre les criminels suivant quatre axes : les sanctions, la forme des sanctions - monétaire ou non-monétaire (ex. emprisonnement), l'ampleur des sanctions et la probabilité de détecter les contrevenants et d'imposer des sanctions. Il analyse dans son modèle la prise de décision du criminel au moment d'agir en se basant sur le gain espéré du criminel et son aversion au risque (Polinsky & Shavell, 2007). Pierre Kopp, quant à lui,

dresse un portrait de l'évolution de la criminalité économique et des outils de lutte contre celle-ci. Le cadre théorique qu'il propose a le mérite d'intégrer la criminalité individuelle et celle des entreprises. L'auteur présente dans (Kopp, 2003), un modèle simplifié d'analyse de la dissuasion qui ne prend en compte que les éléments qui affectent tous les criminels et qui privilégient les variables qui sont susceptibles d'être modifiées par les pouvoirs publics, notamment, les amendes et les peines de prison. En revanche, le modèle ne donne pas de détails sur le niveau d'abstraction et de formalisme mathématiques (Kopp, 2003). Par exemple, les notions d'utilité et de désutilité y sont présentées amplement sans y rattacher une fonction mathématique concrète. Ce que fait très bien Giovanni Mastrobuoni dans ses travaux sur le comportement optimal du criminel et la désutilité du temps de prison. Ses résultats montrent que la distribution de la désutilité du temps de prison est positivement asymétrique et témoigne, selon l'auteur, d'une dissimilitude dans la «peur de la prison » chez les criminels (Mastrobuoni, 2011). Un phénomène qui est susceptible de dépendre des différences dans le coût d'opportunité du temps passé en prison et par conséquent de l'aversion au risque.

Si tous ces chercheurs s'accordent sur la nécessité d'analyser voire de modéliser l'impact potentiel des sanctions pénales sur la prise de décision du criminel au moment de passer à l'acte, très peu d'articles consultés font la même analyse dans le domaine de la cybercriminalité où l'anonymat est un facteur additionnel qui réduit la peur d'être arrêté. Parmi ce petit nombre d'auteurs, notons la contribution de Brenner (Brenner, 2004) avec son modèle de renforcement des sanctions pénales contre les cyber-crimes. Il propose un système de régulation administrative soutenu par des sanctions pénales qui fourniront les incitations nécessaires pour créer un effet dissuasif. Le gouvernement peut mieux contrôler la cybercriminalité en utilisant un système de sécurité «distribué» qui utilise des sanctions pénales pour obliger les utilisateurs d'ordinateurs et ceux qui permettent l'accès au cyberespace à recourir à des mesures de sécurité raisonnables.

A la lumière des articles consultés sur l'évaluation des coûts de monétisation, plusieurs auteurs ont décrit parfaitement le fonctionnement de cette activité, les rôles des acteurs et les difficultés de monétisation qu'ils rencontrent.

Dans un article consacré à l'estimation de la taille du marché des données, Franklin et al. (Franklin, Perrig, Paxson, & Savage, 2007) utilisent des outils de microéconomie pour mesurer les tendances mondiales concernant les variations de prix et la quantité totale d'hôtes compromis. Il note qu'il

existe des similitudes entre le marché noir des données volées et le marché des biens illicites dans le monde réel (Schneider, 2005) où les vendeurs veulent générer plus de profit et les acheteurs (c'est-à-dire les fraudeurs) recherchent les renseignements de qualité pour un rendement plus élevé et tout est soumis aux forces du marché, de sorte que les prix augmentent lorsque la demande est élevée et diminue lorsque la demande est faible (Winder, 2014). Cet article nous inspire en ce sens qu'il examine les activités illégales de ce marché et les sanctions qui en découlent, mais aussi et surtout parce qu'il établit un lien entre prix des renseignements et rendement. Ce qui va dans le sens de l'orientation de notre recherche. Malheureusement, l'article ne traite pas de la question en profondeur. Il n'établit pas de liens formels entre les autres variables et le profit du fraudeur.

2.5.3 Limites des modèles économiques étudiés

Les modèles économiques que nous avons consultés examinent différents problèmes du marché noir sans toutefois analyser les liens entre les différents paramètres qui caractérisent ce marché, notamment, le prix des renseignements, le profit du fraudeur, les commissions versées aux intermédiaires ou encore les coûts divers. Aussi, les modèles d'évaluation des sanctions et les fonctions de désutilité qui en découlent ne concernent pas la fraude bancaire par hameçonnage. Or, la raison pour laquelle nous étudions ces modèles est de trouver un outil qui aide à déterminer les éléments clés qui favorisent la monétisation et ce, afin d'agir efficacement dans la lutte contre ce fléau.

2.6 Victimisation par hameçonnage bancaire

La dernière catégorie de références que nous avons consultées porte sur la victimisation. Ce thème en soi peut englober différents types d'actions. Et, comme il est au cœur de notre projet de recherche, il importe donc de bien le définir avant de poursuivre.

2.6.1 Définitions de la victimisation

Dans sa thèse de doctorat, Yucedal (2010) recense un certain nombre de travaux de recherche qui ont traité de la question de la victimisation dans le cyberespace. Il définit la victimisation par la cybercriminalité comme étant le fait d'être considéré comme une victime d'infractions où une personne spécifique est la cible et, la victimisation informatique, comme le fait d'être victime d'infractions où les ordinateurs, et non les individus, sont des cibles (Yucedal, 2010). Ces

définitions sont partagées par Moitra pour qui les formes de victimisation dans le cyberespace comprennent les virus informatiques, les piratages, les logiciels espions et les logiciels publicitaires (Moitra, 2005). Wall dans son article «Crime and the Internet» soutient que la victimisation dans le cyberespace peut être regroupée en quatre catégories légales :

- la cyber-intrusion : elle réfère à l'accès non autorisé à des réseaux informatiques causant ainsi des dommages. Ces types d'activités consistent en un piratage/craquage, une diffusion de virus, des logiciels espions et des logiciels publicitaires;
- les cyber-déceptions/vols : ils décrivent les crimes conventionnels tels que le vol, la fraude ou le piratage numérique qui se déroulent dans le cyberespace;
- la cyberpornographie : c'est « la publication ou le commerce de matériel sexuellement expressif dans le cyberespace »;
- la cyber-violence : elle fait référence aux activités violentes qui nuisent psychologiquement et/ou physiquement à d'autres personnes et/ou groupes de personnes en violant les lois qui protègent les individus et les groupes. Ces types d'activités violentes consistent en un discours haineux, un cyber-harcèlement, etc. (Wall, 2001).

Plus récemment, S. Perrault (2013) dans son article sur «Les incidents auto-déclarés de victimisation sur Internet au Canada» définit la victimisation sur Internet comme étant soit de la cyber-intimidation, soit un leurre d'enfants, soit une fraude bancaire par Internet, soit des problèmes concernant les achats en ligne, soit de l'hameçonnage et pour chacun de ces incidents, il explique ce que cela signifie. Par exemple, pour une victime de fraude bancaire par Internet, il décline la définition suivante : « Au cours des 12 mois précédant l'enquête, un utilisateur d'Internet s'est servi d'une carte de crédit ou de débit (ou des détails de la carte) pour effectuer des achats ou retirer des fonds du compte sans l'autorisation du détenteur de la carte ». Il en fait de même pour une victime d'hameçonnage. Il la définit comme suit : « A déjà reçu des courriels frauduleux d'une personne se faisant passer pour un représentant d'une organisation fiable et légitime, et demandant des renseignements personnels. Les autres types d'hameçonnage ne sont pas inclus dans le présent article ».

2.6.2 Limites des définitions de la victimisation

À la lumière de ces définitions, on se rend compte effectivement qu'il n'y a pas qu'une forme de victimisation par hameçonnage mais plusieurs. Elle dépend, entre autres, de la technique d'hameçonnage utilisée. Par exemple, pour l'hameçonnage vocal «*Voice Phishing*», la victimisation prend un sens différent du «phishing» par courriel ou par SMS. Ce manque de précision de la littérature sur la définition de la victimisation peut s'expliquer par le fait que, d'une part, les techniques d'hameçonnage sont en constante évolution et, d'autre part, la participation et le rôle de la victime (ex. son comportement en ligne) dans le processus de victimisation changent la donne. Autant sur le plan technique d'hameçonnage que sur le plan humain (victime), cette limite soulève la question de savoir quels sont les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire ?

2.7 Discussion

La littérature sur la fraude bancaire par hameçonnage est très riche et diversifiée. Dans ce travail nous avons regroupé les références consultées en cinq grandes catégories, notamment :

- les définitions;
- les techniques utilisées;
- les contremesures;
- le marché noir (forums clandestins);
- la victimisation.

De la première catégorie, il en ressort que cinq concepts sous-tendent la fraude bancaire par hameçonnage. Il y a la fausse représentation, l'usurpation, la dissimulation, la falsification et le marché noir. Quant au concept de l'anonymat, il n'est pas toujours mentionné explicitement dans les références que nous avons consultées et, pourtant, il est indissociable des activités de la cybercriminalité.

Pour ce qui est de la deuxième catégorie, l'examen de la littérature révèle que les techniques d'hameçonnage utilisées croissent au rythme d'apparition de nouveaux médias et de nouvelles applications (téléphone, SMS, navigateur web, gestionnaire de contact, réseaux sociaux, etc.).

Pour les contremesures, les résultats démontrent que les différentes approches proposées par le passé sont toutes réactives par nature et ont toutes des limites. La première limite identifiée concerne les filtres anti-hameçonnage. Il s'agit du taux d'erreurs de ces filtres et les conséquences sur la confiance de l'utilisateur envers ces filtres. Cette limite soulève la question de savoir quelles améliorations peut-on apporter à ces filtres anti-hameçonnage afin de réduire les taux d'erreurs (ex. faux positifs ou faux négatifs) ?

La deuxième limite concerne la confusion que créent la diversité des outils de gestion des navigateurs, des outils de gestion des mots de passe et l'absence de standard dans les navigateurs. Cette limite nous emmène à nous demander si une standardisation des outils de navigation et des outils de gestion des mots de passe réduirait le risque d'hameçonnage ?

La troisième limite concerne les mises à jour en temps réel des listes de restriction et des fichiers de journalisation. Cette limite peut être déclinée en trois sous-problèmes. Tout d'abord, il y a le problème de limitation des pouvoirs juridiques lorsque vient le moment de collaborer (à l'intérieur d'un pays et en dehors de ses frontières) pour mettre à jour voire supprimer rapidement les listes de sites malveillants. Ensuite, il y a un facteur purement humain. Et, enfin, il y a la nécessité de réagir rapidement, l'âge moyen des sites d'hameçonnage variant de quelques heures à quelques jours seulement (Purkait, 2012). Relativement à ces trois sous problèmes, nous posons, dans cette thèse, la question de savoir si un cadre juridique contraignant visant à favoriser l'échange des listes noires entre partenaires à l'intérieur d'un même pays et avec d'autres pays diminuerait-elle le temps de mise à jour des listes noires.

En ce qui concerne les listes blanches, le premier problème soulevé par l'examen de la littérature est que l'utilisateur peut ne pas respecter les messages d'alerte que lui renvoie le système, auquel cas, il peut se retrouver en train de visiter les sites malicieux, c'est à dire prendre plus de risque. Cette limite soulève la question fondamentale de l'attitude de l'internaute face aux messages d'avertissement des contremesures de sécurité :

> Qu'est-ce qui explique qu'un internaute va prendre en considération ces messages et un autre va les ignorer.

Deux autres limites sur les contremesures ont été évoquées dans la littérature. Il y a la nécessité d'avoir des connaissances préalables sur l'authenticité des sites, sur la contrefaçon des sites et sur l'hameçonnage en général et il y a la négligence en cas de vol de cellulaire ou d'interception des

codes à usage unique envoyés par SMS. Ces deux problèmes renvoient à la question de formation et à la sensibilisation de l'internaute sur les enjeux de sécurité.

Cette question nous conduit inévitablement aux limites des programmes de formation que nous avons soulevées plus haut. Rappelons que l'une des difficultés majeures est que les formations contre l'hameçonnage ne sont pas renouvelées au rythme de parution des menaces. Or, pour faire face à une menace qui change à un rythme effréné, il faut des programmes de formation et de sensibilisation qui s'ajustent à ces changements. Ce problème se résume à l'importance qu'on accorde aux programmes de formation et de sensibilisation aux enjeux de sécurité informatique dans les organisations. Il découle de ce problème la question de recherche suivante :

> Comment peut-on améliorer les formations et les campagnes de sensibilisation aux enjeux de sécurité ?

Relativement à la sécurisation des transactions bancaires en ligne, le problème principal que nous avons identifié dans les travaux antérieurs est qu'il existe une incompréhension ou un manque de connaissances chez les clients de la manière dont fonctionnent les contremesures opérationnelles mises en place pour sécuriser chaque transaction en ligne. Ce problème nous renvoie, une fois encore, au facteur humain et, par le fait même, à la formation et à la sensibilisation aux enjeux de sécurité.

En ce qui concerne les marchés noirs des renseignements volés par hameçonnage, le problème qui ressort de la revue de littérature que nous avons faite est l'absence des données réelles sur son fonctionnement. Ces données auraient permis d'analyser ces marchés afin de déterminer les facteurs clés sur lesquels agir si l'on veut réduire le risque de victimisation par fraude. En l'absence de ces données, nous nous sommes lancé le défi dans cette thèse de construire un modèle microéconomique qui aide à déterminer ces facteurs clés.

Enfin, par rapport à la victimisation par hameçonnage bancaire, l'examen de la littérature sur le sujet ne précise pas la nature de l'incident pour lequel on peut se considérer victime et, encore moins, les circonstances de survenance de cet incident. Pour des fins de cette recherche, nous proposons dans notre approche de réduction du risque un cadre de définition de la victimisation en nous inspirant en partie de chacune des définitions de Wall et S. Perreault. Aussi, la victimisation est utilisée dans cette thèse avec un sens différent du sens le plus courant. Il est le fait de devenir une victime, et non pas simplement de se considérer comme une victime.

2.8 Conclusion : Approche d'analyse et de réduction de risque proposée

Dans ce chapitre, nous avons dressé un portrait de l'hameçonnage bancaire et montrer l'ampleur et l'étendue de ce phénomène. Ce portrait révèle que :

- les fraudeurs utilisent des techniques et des stratagèmes très inventifs, diversifiés et sophistiqués;
- le processus de monétisation des renseignements bancaires est très difficile à décrypter et qu'il n'existe pas de modèle microéconomique qui ait analysé ce pan du cybermarché de la criminalité afin de déterminer les paramètres clés.

Le chapitre qui suit décrit l'approche méthodologique que nous avons privilégiée dans ce travail.

CHAPITRE 3 MÉTHODOLOGIE DE RECHERCHE

Ce chapitre présente le cadre méthodologique suivi dans ce travail de recherche. Il s'agit d'une recherche à la fois explicative et exploratoire. Elle est explicative parce que l'hameçonnage bancaire est un phénomène connu et bien décrit dans la littérature. Néanmoins, les raisons qui expliquent son accroissement au fil des ans malgré que les contremesures existent méritent qu'on s'y attarde pour analyser plus en profondeur les facteurs prédicteurs de risque de victimisation.

Elle est aussi exploratoire en ce sens qu'elle investigue de nouvelles conjectures peu connues, en s'inspirant de ce qui se fait en économie du crime traditionnel, pour analyser le comportement économique du fraudeur dans un marché noir des renseignements volés par hameçonnage.

3.1 Étapes de la méthodologie

Notre méthodologie de recherche comprend six étapes. Dans une première étape, nous effectuons une vaste revue de littérature sur les thèmes de l'hameçonnage bancaire et de la victimisation. Cette revue de littérature permet de dresser un portrait de l'hameçonnage bancaire, d'identifier les insuffisances des solutions de lutte proposées, d'en faire une synthèse et de poser notre question principale de recherche. Ensuite, nous nous fixons quatre objectifs de recherche.

Dans une deuxième étape, nous proposons un cadre de définition de la victimisation par hameçonnage bancaire qui s'appuie sur des éléments fondamentaux que sont le l'action posée, l'objet utilisé, les sujets impliqués et la nature des préjudices subis par ces sujets. Nous exploitons ce cadre pour valider trois formes de victimisation par hameçonnage bancaire tirées des travaux de Perrault et al. (Perreault, 2011). Notamment, la victimisation par tentative d'hameçonnage -*réception de messages hameçonnés*-, la victimisation par infection et la victimisation par fraude -*retrait d'argent des comptes de victimes sans leur autorisation*-. Puis, en nous fondant sur ces trois formes de victimisation, nous émettons six hypothèses de recherche.

Dans un troisième temps, nous analysons les facteurs de risque d'hameçonnage bancaire. En raison des difficultés rencontrées dans la recherche des données sur la victimisation par hameçonnage bancaire, nous allons analyser séparément les facteurs inhérents aux deux premières formes de victimisation de ceux liés à la troisième forme. La première sous-étape consiste donc à exploiter

une partie des données de l'Enquête Sociale Générale de Statistique Canada réalisée en 2009 auprès de 19422 canadiens pour déterminer les facteurs de risque qui permettent de prédire la victimisation par tentative d'hameçonnage et la victimisation par infection. Pour cela, nous utilisons deux méthodes statistiques inférentielles : le test de Khi-2 et un modèle de régression logistique que nous développons spécifiquement pour capter des effets de ces facteurs sur la victimisation.

Toutefois, ces données de Statistique Canada ne concernent pas le processus de monétisation qui concourt au retrait de l'argent des comptes des victimes. Pour cette raison et, à défaut d'autres données empiriques sur cette forme de victimisation, nous développons un modèle microéconomique théorique pour analyser ce processus. Pour y arriver, nous comptons étudier à fond le fonctionnement des marchés noirs afin d'identifier les paramètres qui interviennent dans ce processus. L'analyse de ces paramètres se fait dans la seconde sous-étape. Nous y appliquons la règle de maximisation du profit pour étudier le comportement du fraudeur. Afin de tester notre modèle théorique, nous utilisons des données colligées des forums clandestins.

La dernière étape de notre démarche consiste à colliger et à analyser les avis des experts sur les améliorations à apporter aux contremesures afin de pallier les insuffisances identifiées dans la littérature et aussi sur les résultats de simulation de notre modèle théorique. Pour ce faire, une enquête a été menée auprès de 17 experts en sécurité informatique. Les résultats de cette enquête sont analysés et interprétés avec les statistiques descriptives usuelles : la moyenne, l'écart type et le mode et l'analyse de variance ANOVA.

Le reste du chapitre est organisé comme suit. Dans la section deux, nous présentons les données de recherche. La section trois décrit les méthodes d'analyse de données ainsi que l'approche de modélisation et de simulation utilisées pour notre modèle théorique. Nous concluons ce chapitre avec une section sur l'interprétation des résultats.

3.2 Données de recherche multi-sources

Les données utilisées dans cette thèse proviennent de trois sources distinctes :

1. l'Enquête Sociale Générale 2009;
2. les données colligées d'Internet;
3. les données de l'enquête menée auprès d'experts en sécurité informatique.

3.3 Enquête sociale générale 2009

L'enquête ESG a été menée dans dix provinces et trois territoires Canadiens, de février à novembre 2009 auprès de populations âgées de 15 ans et plus. C'est une enquête transversale par échantillon et à participation volontaire. La collecte de données a été effectuée dans les provinces au moyen d'interviews téléphoniques assistées par ordinateur (ITAO). Par contre, dans les territoires, une combinaison des méthodes ITAO et d'interviews en personne assistées par ordinateur (IPAO) ont été utilisées pour la collecte des données. La méthode d'échantillonnage utilisée par Statistique Canada en était une dite par échantillonnage probabiliste (aléatoire).

Un échantillon d'environ 31 510 ménages avait été sélectionné et 19 422 réponses ont été enregistrées, soit un taux de réponse de 61,6%. Les détails de la procédure d'échantillonnage et de la collecte de données sont bien décrits dans la documentation de l'étude (Perreault, 2011).

1. Choix des données d'enquête ESG pour notre recherche

Trois raisons expliquent notre choix d'utiliser les données de l'Enquête Sociale Générale 2009 pour étudier les facteurs de risque dans cette recherche. Premièrement, cette enquête est la seule enquête nationale basée sur les déclarations des victimes qui recueille les informations, à la fois, sur :

- les trois formes de victimisation que nous avons définies dans cette thèse;
- l'utilisation d'Internet, les risques y afférents et la prévention;
- les caractéristiques sociodémographiques et économiques;
- les caractéristiques liées au revenu, à l'emploi et à l'origine. (StatistiqueCanada, 2009).

De plus, cette enquête recueille des informations sur les conséquences de la victimisation et les décisions prises par les victimes concernant les contremesures de sécurité sur Internet.

Deuxièmement, c'est une très vaste enquête. Une des rares du genre sur la victimisation qui a été menée auprès des dizaines de milliers de Canadiens répartis sur l'ensemble du territoire. Aussi, elle fait partie d'un programme de l'Enquête Sociale Générale menée tous les cinq ans par Statistique Canada depuis 1985 et dont les données ont servi à étayer d'importants programmes du gouvernement afin d'améliorer le bien-être des Canadiens (StatistiqueCanada, 2009).

Troisièmement, dans l'édition ESG 2014, Statistique Canada a retiré le volet des questions relatives à l'utilisation d'Internet, aux risques y afférents et à la prévention. Conséquence, nous ne disposons pas d'une autre enquête d'une telle envergure pour ce volet de notre recherche.

Le volet de l'enquête ESG 2009 sur la victimisation par Internet que nous comptons exploiter dans cette thèse a été utilisé, entre autres, dans deux publications. La première publication, celle de Samuel Perreault et al., utilise ces données pour étudier les caractéristiques liées à la victimisation et les décisions prises par les victimes concernant la déclaration des incidents à la police (Perreault & Brennan, 2010). Le second, Odadas et al. (Odabas, Holt, & Breiger, 2017), l'exploite pour analyser les relations entre les variables démographiques, les perceptions du risque et les activités de routine en ligne sur le vol d'identité, la fraude des consommateurs et la victimisation par hameçonnage.

2. Type et format de données

Le jeu de données de l'enquête contient 55 groupes de variables et 1054 variables en tout. Nous utilisons pour cette recherche 25 variables tirées de neuf groupes, notamment les groupes :

a) renseignements démographiques;
b) revenus;
c) niveau de scolarité du répondant;
d) renseignements géographiques;
e) identité autochtone;
f) langue;
g) minorité visible;
h) utilisation d'Internet et les risques encourus;
i) victimisation sur Internet.

Quant aux 25 variables que nous utilisons, elles sont décrites à l'annexe B. Ces variables sont, pour la grande majorité d'entre elles, qualitatives et pour quelques-unes quantitatives. Les variables qualitatives ont toutes été codifiées par Statistique Canada et sont toutes de type discret. Parmi ces variables plusieurs sont catégorielles. Nous avons effectué une recodification de certaines d'entre elles, notamment, des variables relatives :

- au revenu (cf. Tableau C.1, INCM);
- à l'emploi (cf. Tableau C.5, ACMYR);
- à l'état civil (cf. Tableau C.6, MARSTAT);

- à l'utilisation d'Internet (cf. Tableau C.2, IRP_Q115_C, IRP_Q130_C, IRP_Q135_C, Tableau C.3, IRP_Q160, IRP_Q170);
- à la victimisation par hameçonnage (cf. Tableau C.3 ANNEXE B, IRP_Q243, IRP_Q240, IRP_Q270, IRP_Q300);
- aux contremesures de sécurité (cf. Tableau C.3, IRP_Q340, IRP_Q360, IRP_Q370, IRP_Q380, IRP_Q385, IRP_Q390_1);
- au niveau de scolarité (cf. Tableau C.4, EDU).

Cette recodification a pour objectif d'obtenir un nombre de catégories pertinentes au point de vue de l'analyse et statistiquement maniable. Par exemple, en réduisant le nombre de catégories de la variable revenu de douze à trois, nous définissons ainsi trois classes de revenus : les riches, la classe moyenne et les pauvres. Cette catégorisation a ainsi plus de sens pour notre travail de recherche. Il en est de même des autres variables re-codifiées.

3.4 Données colligées d'Internet

En raison des difficultés rencontrées dans la recherche des informations sur la monétisation des renseignements dans un marché noir, nous colligeons les données d'Internet et, dans certains cas, nous réutilisons les données déjà exploitées dans les travaux de recherche antérieurs, notamment les publications de Florêncio et al. (2010) et de N. Kshetri (2010) et de Wueest (2015). Ces informations sont utilisées pour valider le modèle microéconomique développé au chapitre 6. Il s'agit des informations sur la probabilité de se faire arrêter, le niveau de sécurité que procurent les contremesures, le prix du renseignement et le montant de la commission versé à la mule. Par exemple, à défaut de disposer des chiffres plus récents sur la probabilité (p) de se faire arrêter, nous utilisons des chiffres issus du livre de N. Kshetri (Kshetri, 2010). On peut y lire que la proportion de vols d'identité est estimée à moins 1 sur 700 tandis que le FBI estime la probabilité d'être condamné à 1 contre 22,000.

Relativement au niveau de sécurité (β) mis en place par les banques, nous avons choisi d'utiliser la valeur correspondante au rapport de détection de la fraude bancaire réalisée par les contremesures d'arrière-plan (back-end) et tirée de Florêncio et al, soit 90% de détection de fraudes bancaires réalisées grâce aux contremesures de sécurité (Florêncio & Herley, 2010).

Quant au prix d'achat de chaque renseignement. Il varie entre 0.40 $ et 100 $. Ces chiffres sont tirés de l'article de (Wueest, 2015). 40c correspond à un renseignement de moins bonne qualité alors qu'avec 100 $ on peut se procurer un renseignement d'excellente qualité. La qualité ici fait référence à l'effet combiné de l'origine (américaines vs européennes) et du type du renseignement (AMEX, VISA), des options qu'il offre (platine, or, etc.), de sa durée sur le marché, du solde disponible, du code de sécurité et des informations personnelles du détenteur. Plus un renseignement comprend tous ces éléments, meilleure est sa qualité.

Enfin, il y a la commission versée à la mule (w), c'est un pourcentage (%) du montant total soutiré du compte (R) que le fraudeur verse en contrepartie au service de monétisation que lui rend la mule. Il est compris entre 0.07 et 0.4 fois le revenu anticipé (R). Ces chiffres nous proviennent de l'article de C. Wueest (Wueest, 2015).

3.5 Données de l'enquête menée auprès d'experts en sécurité

Une enquête va être menée auprès des experts pour colliger leurs opinions relativement à deux aspects de notre recherche. Dans un premier temps, nous voulons confronter les opinions des experts avec les résultats d'analyse de notre modèle théorique de monétisation. Ensuite, nous souhaitons obtenir leurs opinions sur les améliorations à apporter aux contremesures afin de pallier les insuffisances identifiées dans la revue de littérature.

3.5.1 Questionnaire

Il comprend quatre parties. Il y a une première partie qui porte sur des questions d'ordre général, notamment, le genre, l'âge, la profession, les champs d'expertise, le nombre d'année d'expériences en sécurité informatique et notamment dans la lutte contre l'hameçonnage bancaire. Ces informations permettent d'analyser les réponses eu égard au profil de l'expert. Ces données seront conservées pour une période d'un an après la fin de l'enquête et après ce délai, elles seront détruites.

La deuxième partie du questionnaire (partie A) vise à identifier les facteurs probables qui influent sur le processus de monétisation dans un marché noir. Les réponses des experts aux questions posées dans cette partie permettent de valider les résultats d'analyse réalisés avec le modèle microéconomique que nous avons développé.

La troisième partie du questionnaire (partie B) vise à colliger les propositions d'améliorations des contremesures identifiées dans la revue de littérature comme étant des facteurs de risque d'hameçonnage bancaire.

Enfin, la dernière partie du questionnaire (partie C) recueille les réponses des experts relativement aux critères de décision à respecter dans le choix des contremesures.

3.5.2 Échelle de mesures utilisée

La mesure des réponses des experts est faite sur une échelle de type Likert à cinq choix.

3.5.3 Certificat d'éthique et de conformité

L'enquête a été approuvée par le comité d'éthique de la recherche (CER) de l'École Polytechnique de Montréal (cf. ANNEXE D).

3.5.4 Échantillonnage

Il s'agit d'une enquête à participation volontaire qui a été menée auprès de 17 experts en sécurité informatique, essentiellement âgés de 25 à 64 ans (cf. Figure 3.1), du 17 août au 30 septembre 2017. Parmi ces experts, 15 étaient des hommes et deux des femmes.

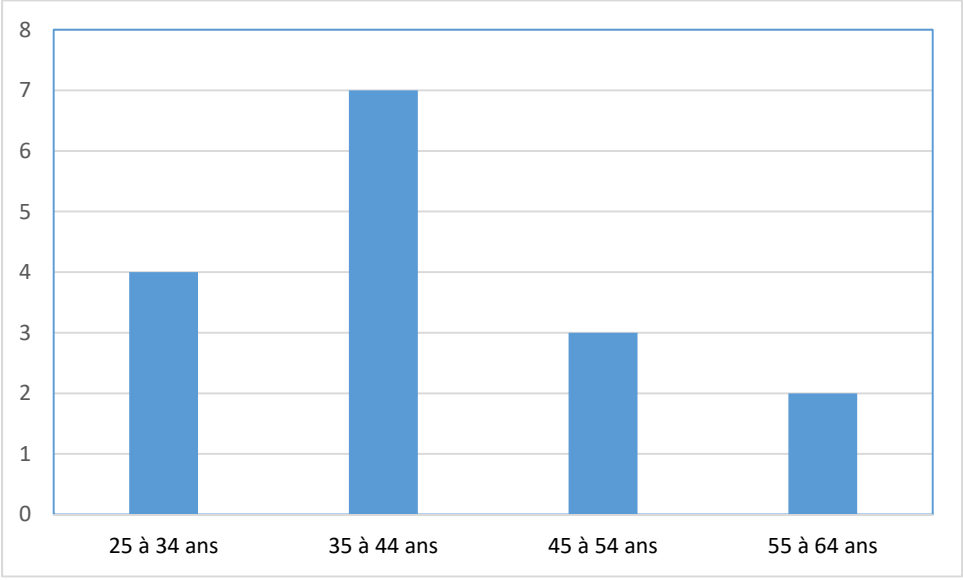


Figure 3.1 : Répartition des experts par groupe d'âge

La sollicitation de ces experts a été faite par courriel couplé à un échange téléphonique.

La méthode de collecte utilisée est dite par échantillonnage raisonné. Les experts sont recrutés dans plusieurs entreprises conseils spécialisées en sécurité informatique, dans deux institutions bancaires et dans trois universités montréalaises comme on peut le voir dans la Figure 3.2 ci-dessous.

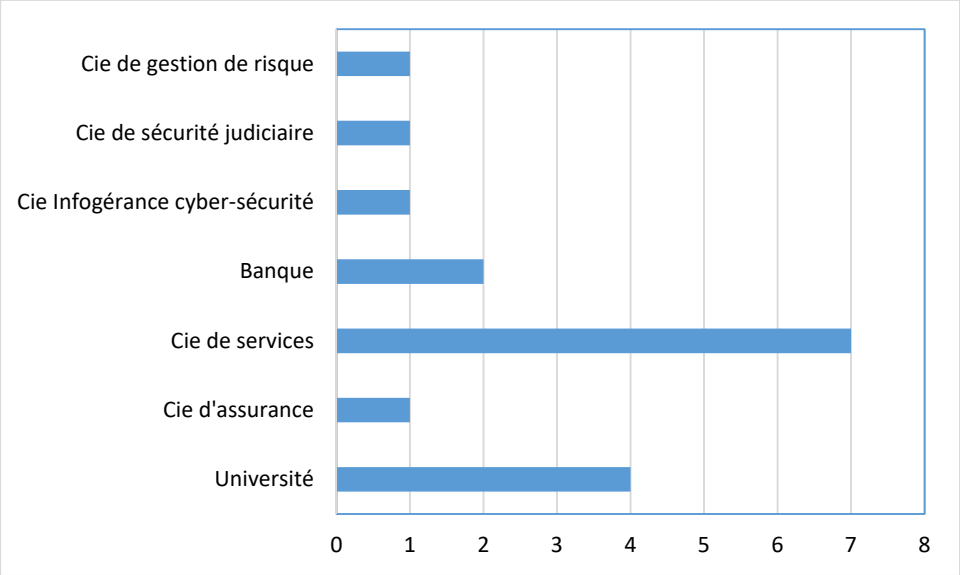


Figure 3.2 : Nombre d'experts par type d'organisation

De la sorte, nous construisons un échantillon représentatif d'experts provenant de sphères différentes et complémentaires. Pour ce faire, 52 experts en sécurité informatique ont été sollicités mais seulement 17 ont répondu favorablement et dans les délais. Nous avons accepté deux experts qui provenaient de la même institution. L'un est gestionnaire et l'autre, un analyste en sécurité.

Tous nos experts sont ou ont été des professionnels en sécurité informatique, de spécialités diverses, cumulant chacun plusieurs années d'expérience ou de prestation dans le déploiement des contremesures de sécurité et, plus spécifiquement, les contremesures de lutte contre l'hameçonnage. La Figure 3.3 ci-dessous nous donne un portrait de différentes spécialités des experts sondés. Les experts ont déclaré près de 10 spécialités.

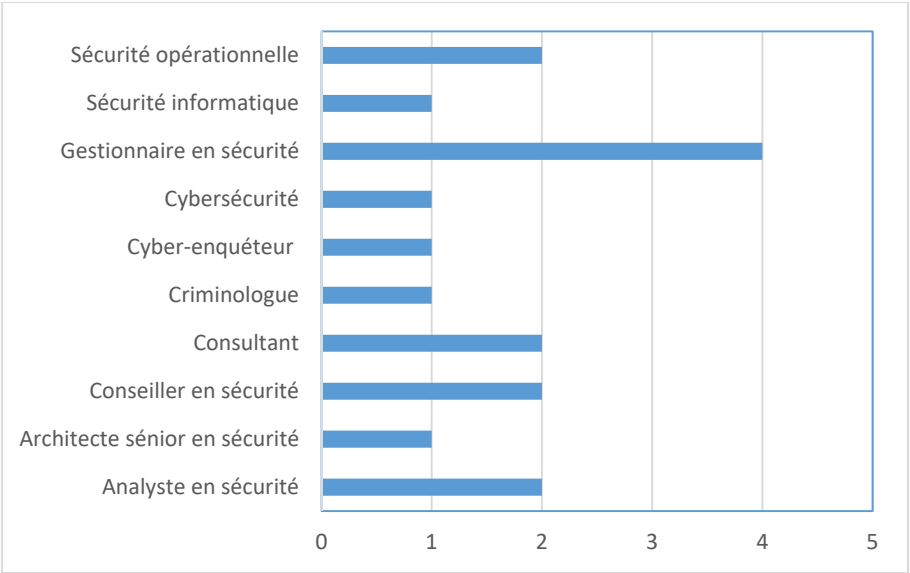


Figure 3.3 : Nombre d'experts par spécialité

Nous avons voulu savoir le nombre d'années en sécurité informatique et notamment en lutte contre l'hameçonnage. Le graphique de Figure 3.4 révèle que 11 personnes sur 17 (65%) avaient une expérience de plus de deux ans dans la lutte contre l'hameçonnage et que sur les 11 personnes, 7 avaient une expérience de plus six ans d'expérience. Enfin, relativement à l'expérience en sécurité informatique, notre échantillon était majoritairement (12 sur 17) formé d'experts ayant plus six ans d'expérience. Ces éléments confirment une chose, l'expérience de ces 17 experts compensait toutefois, nous semble-t-il, leur nombre restreint.

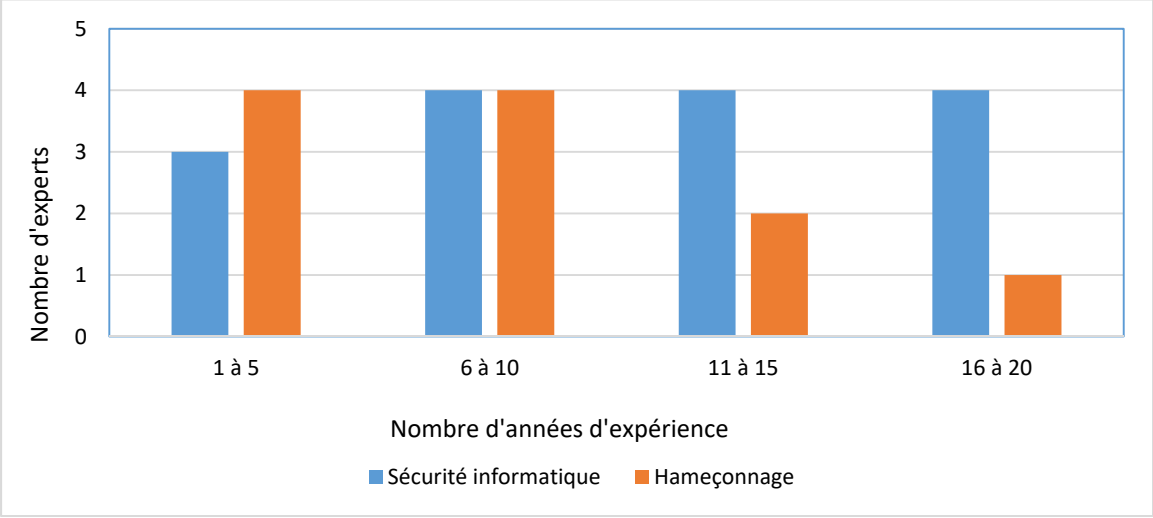


Figure 3.4 : Répartition des experts selon l'expérience

3.5.5 Interprétation des résultats

Les experts ont à choisir les mesures selon leur niveau d'efficacité et sur une échelle de 1 à 5. Le Tableau 3.1 qui suit présente l'échelle d'évaluation utilisée.

Tableau 3.1 : Échelle de l'enquête et interprétation

Choix	Degré d'accord	Signification
1	Très faible	Niveau d'efficacité très bas
2	Faible	Niveau d'efficacité bas
3	Moyen	Niveau d'efficacité moyen
4	Fort	Niveau d'efficacité élevé
5	Très fort	Niveau d'efficacité très élevé
s/o	Sans objet	Sans objet

Pour des fins de cette analyse, les scores cumulés des degrés d'accord «Fort» et «Très fort» seront considérés comme étant un choix favorable à une mesure. En revanche, pour un choix défavorable à une mesure, ce sont les scores cumulés des degrés d'accord «Très faible» et «Faible» qui sont pris en compte.

3.6 Méthodes d'analyses statistiques utilisées

Les données de l'enquête ESG 2009 sont analysées au moyen de deux méthodes statistiques inférentielles. Dans un premier temps, nous utilisons la loi de Khi-2 pour tester des liens probables entre variables indépendantes et variables expliquées et, dans un second temps, nous développons un modèle de régression logistique binaire pour étudier les facteurs qui permettraient de prédire la victimisation.

Quant aux données de l'enquête menée auprès d'experts en sécurité informatique, elles sont analysées à l'aide des statistiques descriptives usuelles : la moyenne arithmétique, l'écart-type et le mode.

a) Statistiques descriptives

Nous utilisons la moyenne arithmétique pour donner la mesure de la tendance centrale des opinions des experts sur les différentes améliorations à apporter aux contremesures. L'écart-type et le mode aident à interpréter ces résultats, le but étant de décrire et d'analyser les résultats observés.

b) Technique des tableaux croisés et le Test de Khi 2

Le test de Khi-2 vise à tester l'hypothèse nulle, c'est-à-dire que les variables indépendantes comme le genre, les revenus, la langue, etc. (cf. Annexe B) n'ont pas d'effet sur chacune des trois variables dépendantes de victimisation par hameçonnage bancaire ci-dessous.

Variables de victimisation

- Tentative d'hameçonnage
  - IRP_Q243 : Problèmes de sécurité. Reçu des courriels frauduleux
- Infection
  - IRP_Q240 : Problèmes de sécurité. Des virus, logiciels espions ou logiciels publicitaires
- Fraude –*retrait non-autorisé de l'argent des comptes des victimes* -
  - IRP_Q270 : Quelqu'un a-t-il utilisé votre carte de crédit ou de guichet à partir d'une source Internet

Pour faire ces tests, nous fixons un seuil de signification à 5%. Ensuite, à l'aide de tableau de contingence, nous éliminons les variables indépendantes dont les liens avec les trois variables de victimisation ci-dessus n'ont pas été établis. Pour les variables dont les liens semblent avérés, rien ne nous indique quelle est la nature de ces liens. C'est donc pour déterminer la nature de ces liens entre variables indépendantes et la victimisation que nous développons un modèle de régression logistique binaire afin d'établir parmi les variables explicatives retenues, celles qui permettraient de prédire la survenue de l'une des trois formes de victimisation que nous venons de définir.

c) Régression logistique binaire

Le choix d'utiliser un modèle de régression logistique binaire se justifie par le fait que chacune des trois variables dépendantes de victimisation est binaire (codée en 0 ou 1), la réponse à chacune des trois questions y afférentes pouvant être un «oui» ou un «non». Le modèle de régression logistique binaire que nous développons dans cette thèse vise à faire des prédictions des variables indépendantes qui sont susceptibles de contribuer à la victimisation tout en capturant les effets combinés des toutes les autres variables explicatives sur la variable expliquée. Aussi, le même seuil de signification à 5% est utilisé.

3.7 Démarche de modélisation et les données de simulation

3.7.1 Démarche

La modélisation que nous réalisons suit un processus en sept étapes.

1. Nous commençons par circonscrire le contexte de l'analyse microéconomique en délimitant le segment du marché noir que nous voulons étudier, c'est-à-dire le marché des renseignements bancaires volés par hameçonnage.
2. Nous définissons notre objectif : étudier les effets des facteurs clés que nous avons identifiés par l'examen des travaux antérieurs, au chapitre deux, sur la monétisation.
3. Ensuite, nous déterminons la variable endogène et les variables exogènes du modèle. La Figure 3.5 ci-dessous montre schématiquement les éléments caractéristiques du modèle à développer. Le modèle reçoit en entrée sept variables exogènes et produit en sortie une seule variable *q*, qui est la quantité de renseignements que le fraudeur est censé monétiser.

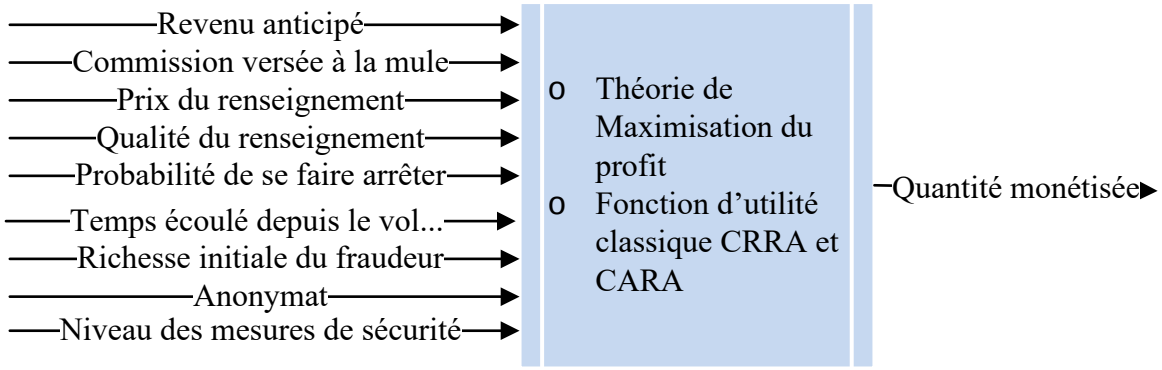


Figure 3.5 : Modèle de monétisation

1. Nous définissons le problème économique de base du fraudeur : la maximisation de l'utilité que lui procurent les renseignements qu'il arrive à monétiser.
2. Afin d'analyser l'attitude du fraudeur vis–à-vis du risque, nous appliquons deux formes fonctionnelles de la fonction d'utilité du fraudeur : la fonction d'utilité classique de type CRRA (*Constant Relative Risk Aversion)* dans le cas où le fraudeur est averse au risque et la fonction d'utilité classique de type CARA (Constant Absolute Risk Aversion) pour le fraudeur qui aime le risque.

3. L'analyse est faite en deux sous-étapes. D'abord, nous utilisons la statique comparative pour étudier les effets de variations des variables d'entrée sur la quantité à monétiser et, par la suite, nous effectuons une simulation de Monté Carlo pour étudier les effets des variations simultanées des variables d'entrée sur la variable endogène. Pour ces simulations, nous utilisons le logiciel MathLab pour la statique comparative et le logiciel d'analyse des risques et décision par simulation de Monte Carlo @RISK de Palissade.
4. Enfin, à la dernière étape, nous interprétons les résultats et nous nous intéressons aux conséquences quant aux contremesures à prendre.

3.7.2 Données de simulation

Les données que nous utilisons pour la simulation sont de deux ordres. Il y a des données fictives utilisées pour des strictes fins de simulation et les données colligées d'Internet. Ces dernières ont été déjà abordées plus haut. Nous les évoquons ici afin d'expliciter les intervalles de valeurs qu'elles vont prendre.

Pour le prix du renseignement, nous utilisons l'intervalle de valeurs T [0.40 $, 0.50 $, 100 $]. 0.40 $ pour la valeur optimiste, 100 $ pour la valeur pessimiste et 0.50 $ pour la valeur probable que le fraudeur est prêt à mettre pour acheter le renseignement.

Quant au niveau de sécurité (β), l'intervalle de valeurs théoriques est compris entre 0.1 et 0.99 - *risque nul n'existant pas*- avec comme valeur probable 90%. T [0.1, 0.9, 0.99]

Les valeurs de la commission (w) payée à la mule sont comprises dans l'intervalle T : [0.07, 0.1, 0.4], la valeur probable, celle qui revient fréquemment dans les articles consultés étant de 10%.

Enfin, nous postulons que la probabilité peut varier de 1/100 à 1/1000 avec 1/700 comme valeur probable, d'où l'intervalle T suivant : T [1/1000, 1/700, 1/100].

Dans la catégorie des données fictives, on retrouve le montant que le fraudeur peut retirer du compte de sa victime (R), les quantités de renseignements que le fraudeur se procure au marché noir en vue de monétiser (Q), la richesse initiale (r) avec laquelle il achète ces renseignements et, le cas échéant, le coût des ressources de clonage nécessaires à la monétisation (b). Nous définissons ci-dessous les intervalles de valeurs pour la simulation.

Pour l'intervalle de valeur de R, nous nous sommes inspirés des données sur les limites de cartes de crédit de Visa issues des sites des banques pour définir l'intervalle de valeurs de simulation entre 500 $ et 10000 $. 500 $ étant la limite de crédit minimale que les banques autorisent, 1500 $ la limite de retrait par jour (valeur probable) et 10000 $ la limite maximale dans notre cas de figure. T [500 $, 1500 $, 10000 $]

Pour la richesse initiale (r), l'intervalle de valeurs est compris entre 40 $ et 1000 $. Il est choisi en se basant sur le prix du renseignement dans les forums clandestins et du nombre de renseignements que nous utilisons pour fin de simulation. L'intervalle T est donc : T [40 $, 50 $, 1000 $]

Enfin, pour les coûts des ressources de clonage (b), une valeur constante arbitraire de 0.50 $ par renseignement est retenue. Aussi, nous supposons que le fraudeur achète la quantité (Q) de 100 numéros d'un coup. Le Tableau 3.2 ci-dessous résume les variables de simulation utilisées ainsi que la loi de distribution et les scénarios utilisés.

Tableau 3.2 : Variables de simulation

Variables	**Loi**	**Scénarios**
R[31]	Triangulaire	T [500 $, 1500 $, 10000 $]
p[32]	Triangulaire	T [1/1000, 1/700, 1/100]
r[33]	Triangulaire	T [40 $, 50 $, 1000 $]
β[34]	Triangulaire	T [0.1, 0.9, 0.99]
w[35]	Triangulaire	T [0.07, 0.1, 0.4]
b	Constante	0.50 $
Q	Constante	100

Le chapitre qui suit propose un cadre de définition de la victimisation par hameçonnage bancaire.

[31] Revenu anticipé du fraudeur

[32] Probabilité de se faire arrêter

[33] Richesse initiale du fraudeur

[34] Niveau de sécurité offert par les banques

[35] Commission versée à la mule pour monétiser

CHAPITRE 4 VICTIMISATION ET HAMEÇONNAGE BANCAIRE : DÉFINITIONS ET HYPOTHÈSES DE RECHERCHE

Dans ce chapitre, nous répondons à notre première question de recherche (Q1[36]) énoncée au chapitre 1. Nous proposons un cadre de définition de la victimisation par hameçonnage bancaire et, pour chaque forme de victimisation identifiée, nous étudions les facteurs de risque qui s'y rapportent avant de formuler les hypothèses de recherche en lien avec nos questions de recherche posées au chapitre 1.

Pour ce faire, nous analysons tout le processus de hameçonnage bancaire. L'intérêt de cette analyse réside dans le fait que tout en décrivant le cheminement d'un hameçon du hacker jusqu'à sa victime, tout en décrivant chaque activité qui concourt ensuite à la fraude bancaire, nous identifions les objets, les sujets (acteurs en présence) et les actions, les liens causaux entre eux et les préjudices subis. Ce qui nous permet, dans une seconde étape, de formuler des hypothèses spécifiques à la question Q2[37] de notre recherche.

4.1 Cadre de définition de la victimisation

Nous proposons un cadre de définition de la victimisation par hameçonnage bancaire qui s'appuie sur un ensemble cohérent d'éléments qui servira de canevas à toute définition de la victimisation par hameçonnage bancaire.

4.1.1 Méthodologie utilisée

Dans notre étude exploratoire, nous avons étudié plusieurs définitions de la victimisation par hameçonnage et de la fraude bancaire tirées des recherches antérieures afin d'identifier les éléments clés qui les caractérisent. Puis, nous avons analysé chaque étape du processus de fraude bancaire par hameçonnage afin de déterminer dans quelles circonstances ces éléments clés s'appliquent ou

---

[36] Q1 Quels sont les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire ?

[37] Q2. Quels sont les facteurs clés de risque de victimisation par hameçonnage bancaire ?

ne s'appliquent pas. Enfin, nous avons recensé dans la littérature les facteurs de risque de victimisation en tenant compte du cadre proposé.

4.1.2 Quelques définitions

1. Victimisation par hameçonnage (Ngo & Paternoster, 2011)

   > Au cours des 12 derniers mois, avez-vous reçu des courriels qui ressemblent à ceux provenant d'entreprises légitimes, y compris des institutions financières ou des organismes gouvernementaux, qui demandent des données personnelles telles que les noms d'utilisateur ou les mots de passe?

2. Victimisation par hameçonnage : (Perreault, 2011)

   > A déjà reçu des courriels frauduleux d'une personne se faisant passer pour un représentant d'une organisation fiable et légitime, et demandant des renseignements personnels.

3. La fraude (Simmons, 1995)

   > La fraude se produit lorsqu'un fraudeur (individu ou organisation) fait intentionnellement une fausse représentation et lorsque la victime (individu ou une organisation), en se fiant à cette représentation, subit des pertes d'argent, de biens ou autre dommage.

4. Victimisation des personnes par fraude (Titus, Heinzelmann, & Boyle, 1995)

   > Ce type de criminalité économique de cols blancs cible les individus et utilise une tromperie dans le but d'obtenir un gain financier illégal. Elle implique la fausse représentation des faits et l'intention délibérée de tromper en promettant des biens, de services ou d'autres avantages financiers qui n'existent pas ou qui ne sont pas tenus.

5. Fraude bancaire par Internet (Perreault, 2011)

   > Au cours des 12 mois précédant l'enquête, un utilisateur d'Internet s'est servi d'une carte de crédit ou de débit (ou des détails de la carte) pour effectuer des achats ou retirer des fonds du compte sans l'autorisation du détenteur de la carte.

Les quelques définitions qui précèdent, et on peut en donner tant d'autres, illustrent la variabilité des définitions de la victimisation par hameçonnage bancaire. Dans les lignes qui suivent, nous analysons chacune de ces définitions afin d'en dégager les éléments clés.

4.1.3 Éléments clés

Il résulte clairement trois éléments des définitions une et deux : il y a la réception du courriel, la non-légitimité du demandeur et la nature des renseignements demandés. Quant aux définitions trois et quatre, elles mettent en lumière la fausse représentation ou tromperie, la victime et les pertes subies. Enfin, la dernière définition met l'accent sur l'action non-autorisée posée par un utilisateur Internet qui se sert des cartes de crédit pour retirer les fonds du compte de sa victime, effectuer des achats, etc.

En résumé, une action :

1. est posée (ex. envoi de message hameçonné, retrait d'argent, capture de renseignements, etc.);
2. utilise un objet : le pourriel, la messagerie instantanée, le téléphone, un logiciel de capture, une pièce jointe, etc. (Aleroud & Zhou, 2017);
3. implique des sujets (ex. les victimes, les attaquants);
4. cause des préjudices de diverses natures.

Avec ces quatre éléments clés qui se dégagent des différentes définitions étudiées, nous allons analyser, dans la section qui suit, chaque étape du processus qui caractérise l'hameçonnage bancaire. Notre objectif est d'identifier à chaque étape quelle est la nature des actions qui sont posées, les objets utilisés, les sujets impliqués et les dommages subis pas ces derniers, le cas échéant.

4.1.4 Analyse du processus d'hameçonnage bancaire

Nous nous sommes inspirés des articles de Hong (2012) et de Qingxiong (2013) pour regrouper les sous-activités relatives à une fraude bancaire par hameçonnage en cinq grandes phases (Figure 4.1). Il y a l'envoi du message hameçonné, sa réception, la compromission de la victime, le vol de renseignements et la fraude en tant qu'action de retirer l'argent du compte de sa victime ou d'effectuer des achats avec ses renseignements (Hong, 2012; Q. Ma, 2013b).

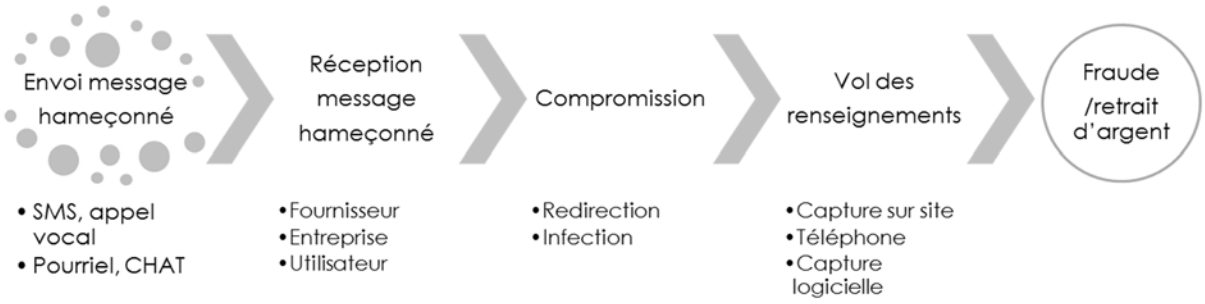


Figure 4.1 : Étapes du processus d'hameçonnage bancaire

4.1.4.1 Envoi de l'hameçon

Nous avons défini cette étape comme le début du processus d'hameçonnage bancaire. En fait, elle correspond aux étapes de planification et d'exécution de l'attaque dans la taxonomie[38] d'Aleroud (Aleroud & Zhou, 2017). L'attaquant planifie son attaque et envoie à « l'aveugle » ou de manière ciblée via des botnets son message hameçonné. Par rapport aux quatre éléments clés de victimisation définis plus haut, l'action ici est l'envoi de message hameçonné ou tentative d'hameçonnage, l'objet utilisé est le SMS ou le courriel ou encore l'appel vocal. Toutefois, il n'y a pas encore de victime et encore moins de dommages.

4.1.4.2 Réception du message hameçonné

Le message hameçonné est généralement reçu par les fournisseurs téléphoniques (cas des SMS et des appels vocaux) ou par des fournisseurs Internet lorsqu'il s'agit des pourriels, des messages instantanés et de fausses sollicitations faites sur les sites web.

Ensuite, ce message chemine à travers les routeurs (Gateway dans le cas du téléphone) d'entreprise, puis est stocké sur un serveur avant d'être téléchargé par l'utilisateur. Dans le cas d'un hameçon vocal, l'utilisateur répond à l'appel téléphonique. Comme on peut le remarquer sur la Figure 4.2 ci-dessous, la réception de message hameçonné se fait à trois niveaux : le niveau fournisseur, celui de l'utilisateur et, le cas échéant[39], le niveau de l'entreprise.

---

[38] Cette taxonomie comprend 3 grandes phases, notamment la phase de planification, la phase d'exécution et la phase d'exploitation des résultats de l'attaque.

[39] Au cas où l'utilisateur

Figure 4.2 : Réception de message hameçonné

Relativement aux quatre éléments clés de victimisation que nous avons définis plus haut, l'objet utilisé demeure inchangé par rapport à la phase d'envoi. En revanche, par rapport à l'action posée, aux sujets et aux préjudices subis par ceux-ci, la réception des messages hameçonnés oblige les fournisseurs et entreprises, le cas échéant, à mettre en place une infrastructure et des ressources pour filtrer ces messages. Ce qui entraîne un coût que nous qualifions dans ce travail de coût de messages reçus mais non-sollicités (appels non sollicités ou courriels indésirables). Au niveau de l'utilisateur, les préjudices sont de trois ordres. Il y a tout le temps qu'il perd à filtrer les messages non-sollicités et qui est difficile de chiffrer, il y a le coût des anti-spams qu'il est obligé de se procurer et il y a le préjudice psychologique que causent, par exemple, toutes ces publicités non-sollicitées, etc. Le tableau 4.1 résume les quatre éléments caractéristiques que nous utilisons pour définir la victimisation subie suite à la réception de messages hameçonnés. Il y a l'action posée, l'objet utilisé, le sujet impliqué et le préjudice.

Tableau 4.1 : Éléments clés de victimisation à la réception du message hameçonné

Action	**Objet**	**Sujet**	**Préjudice**
Réception de message hameçonné/tentative d'hameçonnage réussie	- Pourriel - SMS - CHAT - Appel téléphonique	Fournisseur et Entreprise	- Coût[40] des messages reçus mais non-sollicités - Coût des anti-spams
		Utilisateur	- Coût des anti-spams - Perte de temps (difficile à chiffrer) - Dommage psychologique (dû au harcèlement des utilisateurs)

[40] Coûts en prévention (mise en place des infrastructures et des filtres anti-spam) et coûts en réaction (formation, resserrement des filtres, nettoyage des spams, etc.)

4.1.4.3 Compromission

La compromission survient lorsque l'utilisateur « *mord à l'hameçon* », c'est-à-dire lorsqu'il prend les mesures suggérées, par exemple, en cliquant sur l'hyperlien fictif contenu dans le message hameçonné ou qu'il ouvre une pièce jointe infectée. Plusieurs cas de figure peuvent alors se produire selon que le stratagème utilisé par «l'hameçonneur» soit la tromperie ou l'infection.

4.1.4.4 Tromperie

Premier cas de figure : l'hyperlien conduit à un site falsifié et, comme ces sites falsifiés ressemblent fortement aux sites légitimes, l'utilisateur non avisé saisit ses renseignements personnels et le tour est joué.

Le second cas de figure ressemble au premier mais à la différence que le site web falsifié peut contenir un script qui exploite les failles de sécurité du navigateur de l'utilisateur. Dans ce cas, l'URL du site légitime s'affiche, mais le contenu du site Internet vient d'un serveur trompeur. Le site web légitime affichant des champs de saisie falsifiés trompe la vigilance de l'utilisateur. La suite est similaire au cas de figure précédent.

Le troisième cas de figure utilise les fenêtres contextuelles pour tromper la vigilance de l'utilisateur. L'hyperlien conduit au site web légitime, toutefois, une autre fenêtre du navigateur s'ouvre au premier plan invitant l'utilisateur à saisir ses renseignements personnels. Il est alors difficile, pour quiconque n'est pas assez vigilant, de distinguer la vraie de la fausse fenêtre.

Le quatrième cas de figure ressemble au premier cas sauf que le criminel remplace l'hyperlien trompeur dans le pourriel par un numéro de téléphone du service à la clientèle de l'organisme dont on usurpe l'identité et où la victime présumée devrait appeler.

Enfin, le dernier cas consiste à appeler la cible potentielle et lui demander d'appeler à un numéro de service où il devrait fournir ses renseignements pour éviter un supposé problème (K. Choi et al., 2017).

4.1.4.5 Infection

On en distingue deux formes : soit le logiciel espion est installé à la suite d'un clic sur une pièce jointe infectée ou dans une fenêtre pop-up, soit par un «drive-by-download[41]». Dans un cas comme dans l'autre, le «hameçonneur» fait en sorte que ce soit l'utilisateur lui-même qui télécharge et installe, à son insu, le programme malveillant sur son ordinateur. Cet état de fait renvoie d'une part, à l'attitude ou à la responsabilité de l'utilisateur et, d'autre part, à l'efficacité des contremesures en place.

À la lumière de cette brève description, nous analysons ci-dessous le processus de compromission eu égard aux quatre éléments clés de victimisation identifiés plus haut. L'action posée consiste à cliquer sur un lien ou appeler au numéro de téléphone suggéré dans le message hameçonné. Elle cause des préjudices à l'utilisateur (ex. perte de temps, peur induite par l'action posée, coût de désinfection, le cas échéant) et probablement à l'entreprise et au fournisseur (ex. coût de désinfection).

Tableau 4.2 : Éléments clés de victimisation lié au clic sur l'hameçon

Action	**Objet**	**Sujet**	**Préjudice**
Clic sur un lien ou appel à un numéro /Infection	Pourriel SMS CHAT Appel téléphonique	Fournisseur et Entreprise	Perte de temps (difficile à chiffrer) Coût de désinfection
		Utilisateur	Perte de temps (difficile à chiffrer) Psychologique (peur induite par l'action posée, la culpabilité) Coût de désinfection.

4.1.4.6 Vol ou capture des renseignements

C'est la phase de collecte et de transfert des renseignements bancaires de la machine infectée ou du site malicieux vers les bases de données ou les comptes courriels sur Internet. Elle se fait

[41] *Un dry-by-download* est un logiciel malveillant qui s'installe automatiquement sur ordinateur, à l'insu de l'utilisateur, suite à la consultation d'un mail ou d'un site piégé. Il exploite généralement **une** vulnérabilité des navigateur**s** web ou des mauvais paramétrages de sécurité**.**

généralement par un logiciel de capture d'informations installé dans l'ordinateur de la victime ou à travers des formulaires en ligne. L'action ici est posée soit par l'utilisateur lorsqu'il s'agit de saisir les renseignements sur des formulaires en ligne ou par le logiciel de capture lorsque c'est une infection. Lorsque c'est l'utilisateur qui saisit ces propres renseignements en ligne, l'action est autorisée même comme c'est une tromperie. En revanche, lorsque c'est un logiciel qui capture ces renseignements de l'ordinateur, l'action est non autorisée. La victime ici est l'utilisateur et le préjudice est de trois ordres : perte de temps et peur de s'être fait voler ses renseignements bancaires, coût de désinfection.

Tableau 4.3 : Éléments clés de victimisation liés au vol ou à la capture des renseignements

Action	**Objet**	**Sujet**	**Préjudice**
Saisie /capture les renseignements	- Logiciel - Formulaire en ligne	Utilisateur	- Perte de temps (difficile à chiffrer) - Psychologique (peur induite par l'action posée, la culpabilité)

4.1.4.7 Fraude ou retrait non autorisé des comptes des victimes

La fraude survient lorsqu'il y a retrait non autorisé de l'argent du compte de la victime. L'action est le retrait non autorisé et les objets sont de diverses natures : les renseignements bancaires, les transferts entre comptes, le fraudeur peut aussi faire fabriquer des cartes de crédit ou de débit physiques et s'en servir pour faire ou faire faire des retraits ou encore effectuer des achats. Dans un cas comme dans l'autre, les victimes sont : la banque et/ou les institutions affiliées, l'utilisateur et, dans certains cas, les marchands. Les préjudices sont de natures diverses. Il y a la perte de temps et d'argent de toutes les victimes, il y a un préjudice psychologique ou moral (insomnie, angoisse, anxiété, etc.) causé à l'utilisateur victime, il y a enfin une probable atteinte à la réputation des banques et/ou institutions affiliées. Le tableau 4.4 ci-dessous résume très bien tous les éléments qui caractérisent la victimisation par fraude.

Tableau 4.4 : Éléments clés de victimisation liés au retrait non autorisé

Action	**Objet**	**Sujet**	**Préjudice**
Retirer des fonds du compte	- Achats - Retrait en ligne/guichet /comptoir - Transfert	- Banques - Marchands	- Perte de temps (difficile à chiffrer) - Perte d'argent - Probable atteinte à la réputation (difficile à chiffrer)
		Utilisateur	- Perte de temps (difficile à chiffrer) - Perte d'argent - Psychologique (insomnie, angoisse, anxiété, etc.)

À la lumière de ce qui précède, nous pouvons noter deux enjeux en lien avec la compromission et le vol ou la capture des renseignements.

Tout d'abord, lorsque l'utilisateur clique sur le lien suggéré dans le message hameçonné ou encore lorsqu'il saisit ses coordonnées bancaires dans un formulaire en ligne sur un site malveillant, l'action ne peut être considérée comme «non-autorisée» puisqu'il le fait de son propre chef. À contrario, l'envoi des messages hameçonnés, l'infection de l'ordinateur par un Trojan bancaire, le vol des données à l'aide des «Keyloggers» et le retrait d'argent des comptes bancaires sont bel et bien des actions non-autorisées.

Ensuite, la capture des renseignements par des logiciels est complètement transparente à l'utilisateur. Le préjudice n'est donc par perceptible puisqu'il est confondu au préjudice relatif à l'infection. Au mieux, l'utilisateur va se rendre compte qu'il a été infecté et au pire il ne s'en aperçoit que lorsqu'il y a un autre incident : le retrait non autorisé d'argent de son compte et encore, certains ne le réalisent que lorsqu'ils reçoivent leurs relevés à la fin du mois. Pour des fins de cette recherche, nous avons considéré que cliquer sur un lien, saisir des renseignements en ligne et se faire capter des renseignements par un logiciel constituent des étapes intermédiaires entre d'une part la réception des messages hameçonnés et le retrait non autorisé et, d'autre part, entre l'infection et le retrait non autorisé d'argent du compte bancaire, le préjudice n'étant pas perceptible.

En réponse donc à notre question de recherche Q1, les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire sont les suivants :

Action

- l'envoi des messages hameçonnés
- la réception des messages hameçonnés
- l'appel téléphonique
- la création de site web falsifié
- ouverture de pièce jointe
- rappel d'un numéro
- clic sur un lien
- l'infection d'ordinateur
- le retrait d'argent des comptes bancaires
- la capture de renseignements

Objet

- pourriel
- SMS
- CHAT
- appel téléphonique
- logiciel de capture de renseignement (ex. Keyloggers)
- pièce jointe
- formulaire en ligne
- site web falsifié
- achats en ligne
- Retrait en ligne/guichet /comptoir
- transfert entre comptes

Sujet

Victime

- Fournisseurs de services Internet et de services téléphoniques
- Entreprises
- Utilisateurs
- Banques
- Marchands

Attaquant

- mules
- hackers
- intermédiaires

Préjudice subi

- coût des messages reçus mais non-sollicités (coût en prévention, cf. Tableau F.1)
- coût de désinfection (coût en conséquence, cf. Tableau F.1)
- perte de temps (difficile à chiffrer)
- psychologique (souffrance morale, peur, insomnie, angoisse, anxiété, la culpabilité)
- perte d'argent
- probable atteinte à la réputation (difficile à chiffrer)

4.1.5 Conclusion

Les quatre catégories d'éléments clés que nous venons d'identifier constituent le canevas que nous proposons pour toute éventuelle définition de la victimisation par hameçonnage bancaire (cf. Figure 4.3). Une définition de la victimisation par hameçonnage doit contenir des éléments de chacun de ces catégories.

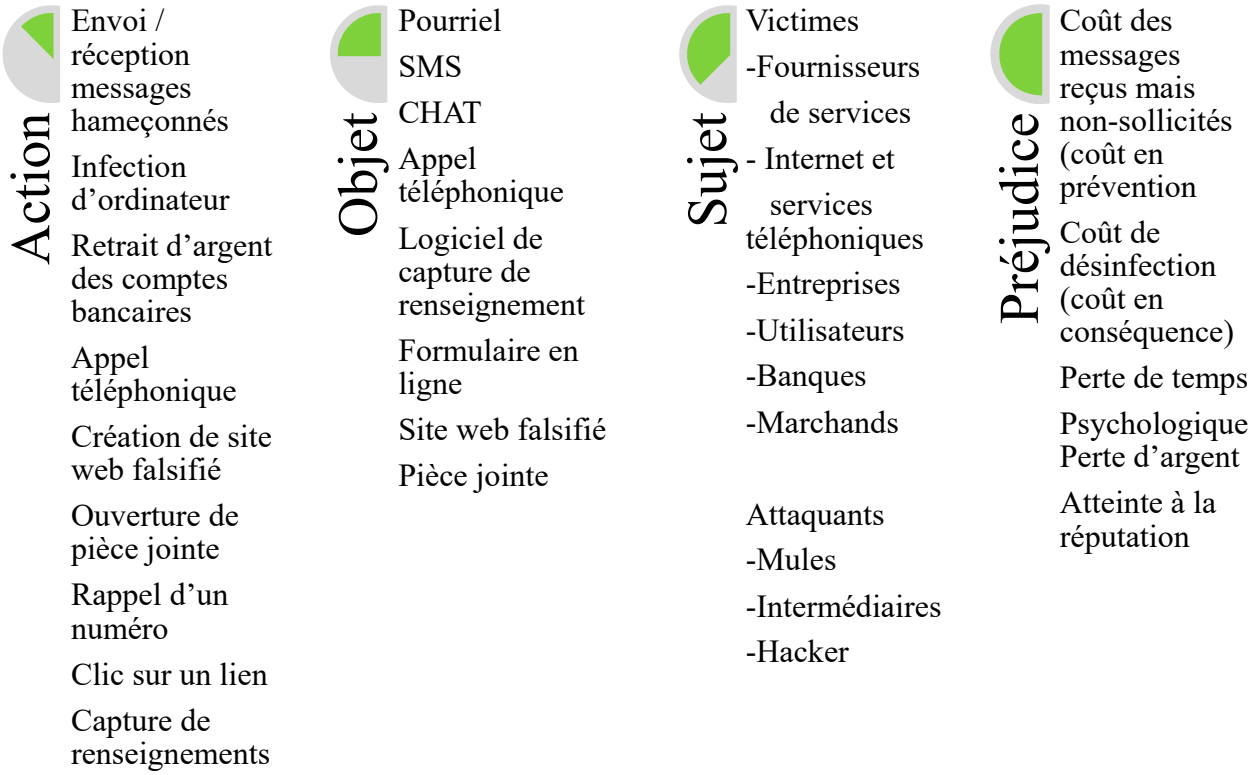


Figure 4.3 : Cadre de définition de la victimisation proposé

La section qui suit présente les facteurs de risque d'hameçonnage fondé sur ce cadre de définition.

4.2 Facteurs de risque de réception de message hameçonné

L'action dans ce cas est la réception de message hameçonné et le problème fondamental que cette réception pose est de savoir comment empêcher que cette action se produise ou, à tout le moins, en réduire les impacts. Pour aborder le problème, il faut déjà identifier les facteurs de risque sur lesquels agir, le cas échéant. Et c'est en sens que la question plus générale Q2[42] de notre recherche a été adressée.

La littérature consultée révèle qu'il y a deux types de facteurs qui expliqueraient que malgré la présence des contremesures sur les systèmes des fournisseurs, des entreprises et des utilisateurs, des messages hameçonnés parviennent quand même à la victime. Il y a des facteurs humains et ceux inhérents aux limites de certaines contremesures.

4.2.1 Facteurs humains

Muchang et al. donnent un exemple de facteur relevant de la responsabilité de l'utilisateur qui contribue à exposer ce dernier et les autres victimes à la réception des messages hameçonnés. Ils soulignent le lien entre le fait qu'un internaute porte une attention aux avertissements de sécurité générés par les barres d'outils et la réception des messages hameçonnés. Pour ces auteurs, ceux qui ne lisent pas les avertissements acceptent souvent des invitations qui les rendent plus susceptibles d'être la cible des «hameçonneurs» que ceux qui font plus attention (Muchang et al., 2015). Toutefois, ils n'expliquent pas les raisons pour lesquelles un internaute va prendre en considération les messages d'avertissement de sécurité et un autre va les ignorer.

Furnell et al. abondent dans le même sens lorsqu'ils révèlent que les problèmes de la journalisation des sites malveillants sont en partie liés à l'humain qui ne prend pas toujours les dispositions nécessaires pour que les fichiers de journalisation soient mis à jour en temps réel (Furnell et al., 2008). D'autres recherches antérieures ont montré que certains comportements en ligne de l'utilisateur contribuent à l'exposer aux menaces et à en faire une cible de messages hameçonnés.

Pour toutes ces raisons, il est raisonnable d'émettre des hypothèses sur les liens probables entre d'une part, les caractéristiques sociodémographiques et économiques et le fait de recevoir des

[42] Q2. Quels sont les facteurs clés de risque de victimisation par hameçonnage bancaire ?

messages hameçonnés et, d'autre part, entre les comportements qu'adoptent les utilisateurs en ligne et le fait de recevoir des messages hameçonnés. Par comportements, on entend la manière et la fréquence d'utilisation d'Internet et de certains services en ligne (Hutchings & Hayes, 2008), notamment :

L'utilisation d'Internet pour les transactions impliquant des renseignements bancaires

- les services de paiement, de réservation et d'achat en ligne
- les services Internet pour effectuer des opérations bancaires électroniques

L'utilisation d'Internet pour socialiser

- les sites de réseautage social
- les salons de clavardage

Afin de répondre au volet des facteurs humains de la question Q2 de notre recherche, nous avons émis les hypothèses suivantes :

H4.1.a : L'utilisation d'Internet pour effectuer les transactions impliquant les renseignements personnels augmente la probabilité de recevoir des messages hameçonnés;

H4.1.b : La fréquentation des réseaux sociaux et des salons de clavardage augmente la probabilité de recevoir des messages hameçonnés.

4.2.2 Facteurs liés aux limites de certaines contremesures

Les limites des contremesures relatives à la réception des messages hameçonnés que nous avons relevées dans notre revue de littérature concernent les filtres anti-hameçons, les navigateurs, la mise à jour des fichiers de journalisation et des listes de restriction. Moore et al. proposent que pour empêcher que les messages hameçonnés parviennent aux victimes, il faut supprimer en temps réel tous les sites d'hameçonnage dès qu'ils sont détectés (Tyler Moore & Clayton, 2007). Ce qui n'est pas toujours le cas. Parmi les raisons invoquées par ces chercheurs pour justifier cet état de fait, il y a les limites du cadre juridique actuel entre pays et les limites dans la collaboration entre organismes à l'intérieur d'un même pays (ex. hébergeurs de site web et fournisseurs Internet). D'autres travaux font le même constat. Ce qui nous pousse, dans cette thèse, à nous interroger sur

la nécessité d'avoir un cadre juridique qui permettrait un échange rapide d'informations entre partenaires (Q5[43]).

Notre démarche de recherche étant exploratoire, l'enquête que nous allons mener auprès des experts en sécurité informatique permettra de répondre à cette question au chapitre 7 de cette thèse.

4.3 Facteurs de risque d'infection

Le second type d'action que nous avons identifié dans notre cadre de définition de la victimisation et pour lequel une victime estime avoir subi des préjudices est l'infection de l'ordinateur par un Trojan bancaire. Le problème que pose cet incident est similaire à celui que nous avons relevé pour les facteurs de risque de recevoir les messages hameçonnés, à savoir, comment empêcher que l'infection se produise ? Cette question porte sur un aspect de la problématique plus large que nous avons formulée dans notre question de recherche Q2 relative aux facteurs de risque de victimisation.

Selon Arachchilage et al., l'infection d'un système par hameçonnage serait très souvent due à trois situations indésirables (Arachchilage & Love, 2014) :

- l'anti-virus ou l'anti-spam est défectueux ou absent;
- les filtres anti-hameçonnage sont déficients ou absents;
- les navigateurs sont mal ou pas du tout sécurisés.

D'autres recherches antérieures ont révélé que le manque de formation ou de sensibilisation aux enjeux de sécurité pouvait être un facteur de risque d'infection. Parmi ces recherches, il y a les articles d'Arachchilage (2014) et Liang (2010) qui soulignent que plus l'utilisateur final est formé –sensibilisé- aux enjeux de sécurité, moins il est susceptible de se faire infecter par hameçonnage. À contrario, l'utilisateur qui n'est pas formé –sensibilisé- aux enjeux liés à la sécurité informatique,

- n'arrive pas à distinguer un site falsifié (usurpé) d'un site légitime,

[43] Q5. Un cadre juridique visant à favoriser l'échange des listes noires entre partenaires à l'intérieur d'un même pays et avec d'autres pays diminuerait-elle le temps de mise à jour des fichiers de journalisation ?

- n’arrive pas à repérer un message hameçonné, à identifier un faux lien URL ou un faux formulaire électronique,
- ne supprime pas régulièrement les courriels envoyés par des expéditeurs inconnus,
- ne supprime pas régulièrement les fichiers Internet temporaires,
- utilise des mots de passe faibles et ne les change pas de façon régulière.

(Arachchilage & Love, 2014; Liang & Xue, 2010).

Or, l’examen poussé de la littérature montre qu’il est très difficile d’établir clairement quelle est la cause profonde, par exemple, de la défaillance de l’antivirus ou des filtres anti-hameçons. Est-ce qu’une telle défaillance relève d’une cause purement technologique ou d’un manque de formation/sensibilisation aux enjeux de sécurité ?

Pour cette raison, nous pensons qu’il est important d’analyser les liens de causalité entre certains de ces éléments de risque d’infection afin de dire quels sont véritablement les facteurs de risque d’infection par hameçonnage (Q2).

Nos hypothèses sont donc similaires à celles émises à la phase de réception des messages hameçonnés, excepté qu’elles réfèrent à la phase d’infection.

H4.2.a : L’utilisation d’Internet pour effectuer les transactions impliquant les renseignements personnels augmente la probabilité de se faire infecter;

H4.2.b : La fréquentation des réseaux sociaux et des salons de clavardage augmente la probabilité de se faire infecter.

Les limites des contremesures relatives à l’infection par un Trojan bancaire que nous avons relevées dans la littérature portent sur le taux élevé d’erreurs des filtres anti-hameçonnage, les mauvaises configurations des navigateurs, la gestion des mots de passe et le manque de sensibilisation aux enjeux de sécurité. Plusieurs pistes de solutions ont été proposées dans les recherches antérieures. Parmi ces pistes, il y a l’utilisation de la signature électronique dans le courriel, la standardisation des configurations des navigateurs et des modules de gestion des mots de passe et l’intensification des efforts de sensibilisation aux enjeux de sécurité (Adida et al., 2005; S.-H. Kim et al., 2013; S. Kim et al., 2015). Toutefois, nous n’avons pas trouvé de mesures de l’utilisation et de l’efficacité

de ces solutions. C'est la raison pour laquelle nous avons formulé, dans cette thèse, les questions de recherche Q3[44], Q4[45], Q6[46] et Q7[47] avec pour objectif de recueillir et d'analyser les avis des experts sur la praticabilité de ces solutions et de faire des recommandations.

4.4 Facteurs de risque de retrait non-autorisé d'argent des comptes bancaires

Le troisième type d'action que nous avons identifié dans notre cadre de définition de la victimisation est le retrait non-autorisé d'argent des comptes des victimes. Plusieurs travaux de recherche s'accordent pour dire que le retrait d'argent est l'aboutissement d'un processus de monétisation très complexe et en constante évolution. Ils identifient deux types de facteurs potentiels qui contribueraient au retrait non-autorisé d'argent des comptes des victimes, notamment, les variables liées au marché noir des renseignements et le comportement de l'internaute (Tyler Moore et al., 2009; Holt & Lampke, 2010; Motoyama et al., 2011; Shulman, 2010; Sood et al., 2013).

Relativement aux variables liées au marché noir, Ablon et al. (Lillian Ablon et al., 2014) invoque «l'âge» du renseignement bancaire sur le marché noir. Il explique que le retrait d'argent d'un compte est plus aisé immédiatement après que le vol des données y afférentes ait eu lieu. D'autres recherches antérieures identifient l'efficacité et la disponibilité de la mule chargée de convertir les renseignements bancaires comme le facteur clé qui contribue au retrait de l'argent des comptes des victimes.

Pour Herley (2014), le retrait d'argent des comptes est soumis aux aléas du marché noir et particulièrement aux difficultés inhérentes au processus de monétisation. Herley (2014) explique qu'une des difficultés de monétisation est le caractère réversible des transactions bancaires (ex. annulation possible) qui oblige le fraudeur à avoir recours au service de «mule» pour soutirer de l'argent du compte de sa victime (Herley, 2014).

---

[44] Quelles améliorations peut-on apporter aux filtres anti-hameçonnage afin de réduire les taux d'erreurs (ex. faux positifs ou faux négatifs) ?

[45] Comment rendre les navigateurs plus sécuritaires à l'encontre des pirates ?

[46] Quelle est l'importance accordée aux formations en sécurité et aux campagnes de sensibilisation sur les menaces dans les organisations ?

[47] Comment peut-on améliorer les formations et les campagnes de sensibilisation aux enjeux de sécurité ?

D'autres recherches antérieures consultées sur les marchés noirs des renseignements bancaires montrent que la probabilité de se faire arrêter et d'être sanctionné, le cas échéant, influencerait le retrait d'argent des comptes des victimes. Afin d'y voir plus clair et de déterminer parmi ces variables lesquelles ont une plus grande incidence sur le processus de retrait d'argent des comptes, nous trouvons qu'il est justifié d'utiliser les outils d'analyse micro-économique pour étudier les liens entre toutes ces variables. En ce sens, le chapitre six de notre thèse, tout en analysant le comportement du fraudeur au cours de l'activité de monétisation des renseignements bancaires, aide à déterminer les facteurs réels de risque de retrait d'argent des comptes des victimes.

Pour ce qui est de l'influence du comportement en ligne de l'internaute sur le retrait d'argent des comptes, S. Perrault invoque les liens probables d'une part, entre l'utilisation d'Internet pour effectuer les transactions en ligne et le retrait d'argent du compte et, d'autre part, entre la fréquentation des réseaux sociaux et le retrait d'argent du compte (Perreault, 2011). Nous pensons que des recherches supplémentaires devraient être menées afin de confirmer ou d'infirmer les liens entre de tels comportements en ligne et le risque de retrait d'argent du compte d'une victime. C'est en ce sens que nous avons émis les hypothèses suivantes :

H4.4.a : L'utilisation d'Internet pour effectuer les transactions impliquant les renseignements personnels augmente les risques de retrait non-autorisé d'argent des comptes des victimes.

H4.4.b : La fréquentation des réseaux sociaux et les salons de clavardage augmente les risques de retrait non-autorisé d'argent des comptes des victimes.

4.5 Récapitulation des hypothèses de recherche relatives à la question de recherche Q2

H4.1.a : L'utilisation d'Internet pour effectuer les transactions impliquant les renseignements personnels augmente la probabilité de recevoir des messages hameçonnés.

H4.1.b : La fréquentation des réseaux sociaux et des salons de clavardage augmente la probabilité de recevoir des messages hameçonnés.

H4.2.a : L'utilisation d'Internet pour effectuer les transactions impliquant les renseignements personnels augmente la probabilité de se faire infecter.

H4.2.b : La fréquentation des réseaux sociaux et des salons de clavardage augmente la probabilité de se faire infecter.

H4.4.a : L'utilisation d'Internet pour effectuer les transactions impliquant les renseignements personnels augmente les risques de retrait non-autorisé d'argent des comptes des victimes.

H4.4.b : La fréquentation des réseaux sociaux et les salons de clavardage augmente les risques de retrait non-autorisé d'argent des comptes des victimes.

Pour valider ces hypothèses, nous utilisons les données provenant de l'Enquête Sociale Générale (ESG) ("Statistique Canada, les incidents autodéclarés de victimisation sur Internet au Canada, 2009,") réalisée en 2009 par Statistique Canada auprès de 19422 personnes et qui porte sur la perception qu'ont les Canadiens des crimes perpétrés dans leur milieu, sur leur attitude envers le fonctionnement du système de justice pénale et leurs expériences de la victimisation.

4.6 Conclusion

Nous avons proposé dans ce chapitre, en réponse à notre question de recherche Q1, un cadre de définition de la victimisation par hameçonnage bancaire qui s'articule autour de quatre blocs d'éléments clés.

En premier, il y a la bonne identification du type d'action pour lequel une personne ou une entité morale se considère comme une victime. Ce cadre permet de s'assurer que ce soit une action non-autorisée et qu'elle cause un préjudice perceptible à une personne ou une entité morale.

Ensuite, il y a les moyens utilisés. Ces moyens sont divers et évoluent globalement au rythme de parution des nouvelles technologies de l'information et de la communication. Toutefois, ce qui les caractérise tous, c'est l'absence de contact physique et personnel.

Le troisième bloc d'éléments concerne la victime. Notre cadre analyse le processus d'hameçonnage afin d'identifier à chaque étape importante les victimes potentielles, qu'elles soient une personne physique ou une entité morale.

Enfin, il y a le préjudice. Notre cadre élargit la notion de préjudice pour inclure d'autres formes de préjudices comme la perte de temps et l'atteinte à la réputation.

Le premier bloc du cadre d'analyse et de réduction de risque que nous proposons dans cette thèse est ainsi complété avec les trois formes de victimisation que nous venons de déterminer (cf. Figure 4.4 ci-dessous) à savoir : la réception des messages hameçonnés, l'infection et le retrait d'argent des comptes des victimes.

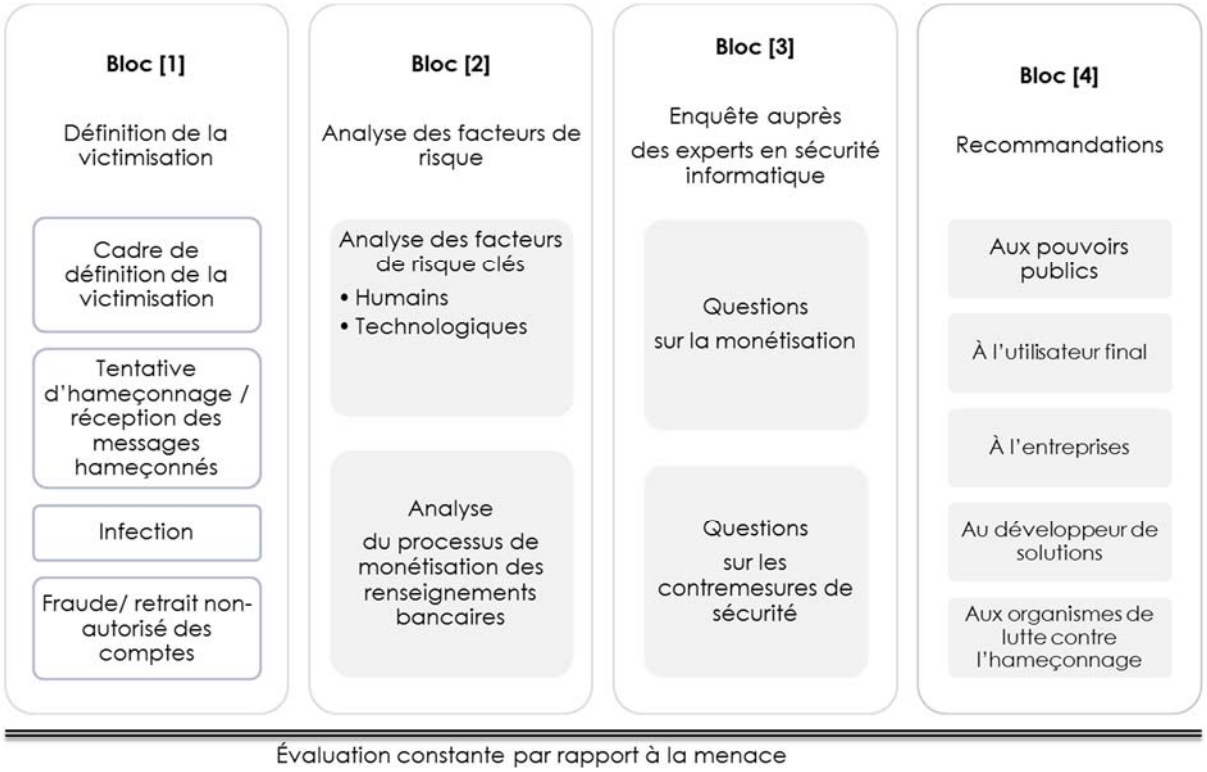


Figure 4.4 : Cadre d'analyse et de réduction de risque d'hameçonnage bancaire proposé

CHAPITRE 5 ANALYSES DES FACTEURS DE RISQUE DE VICTIMISATION PAR HAMEÇONNAGE BANCAIRE

Le chapitre 4 a circonscrit notre champ de recherche à trois formes de victimisation par hameçonnage et permis d'émettre des hypothèses de travail.

Ce chapitre analyse les liens de causalité entre ces facteurs de risque de victimisation en exploitant les données de l'enquête ESG 2009. Nous développons un modèle de régression logistique pour analyser les facteurs de risque multiple et pour déterminer parmi ces facteurs ceux qui permettent de prédire la victimisation par hameçonnage.

Nos résultats d'analyse montrent que l'utilisation d'Internet pour effectuer les achats et les opérations bancaires en ligne est un facteur plus prédicteur de la tentative d'hameçonnage et de fraude que tous les autres facteurs de risque. Pour la victimisation par infection, le facteur de prédiction le plus important est l'utilisation des salons de clavardage suivie, étonnamment, du genre et de l'activité principale de l'internaute.

Les résultats d'analyse du risque moral et du signalement à temps des incidents suggèrent que des études plus poussées, avec des données précises, soient faites sur les impacts de ses facteurs potentiels de victimisation par hameçonnage.

5.1 Notre contribution

L'enquête ESG 2009 a été exploitée entre autres par deux auteurs. Les premiers, Samuel Perreault et al., utilisent les données de cette enquête pour examiner les caractéristiques liées à la victimisation criminelle, y compris les facteurs de risque sociodémographiques, les conséquences de la victimisation et les décisions prises par les victimes concernant la déclaration des incidents à la police (Perreault & Brennan, 2010). Les seconds, Odadas et al. l'exploitent pour analyser les relations entre les variables démographiques, les perceptions du risque et les activités de routine en ligne sur le vol d'identité, la fraude des consommateurs et la victimisation par hameçonnage (Odabas et al., 2017).

Dans ce chapitre, nous confirmons, dans un premier temps, les résultats d'analyse de Perreault et al. avec les mêmes données, puis, à l'aide d'un modèle de régression logistique, nous analysons

les facteurs prédicteurs de victimisation. Mais, l'apport le plus significatif avec ces données de l'Enquête ESG 2009 est, sans aucun doute, l'utilisation de ces données pour tenter d'appliquer la notion d'aléa moral dans le domaine de la sécurité informatique.

Pour la suite du chapitre, les expressions *tentative d'hameçonnage* et *réception du message hameçonné* seront utilisées invariablement.

5.2 Analyse des facteurs de risque individuel[48]

5.2.1 Caractéristiques sociodémographiques

L'analyse des impacts des caractéristiques sociodémographiques étudiées individuellement a produit les résultats que nous avons résumés au Tableau G.1 et, que nous vous présentons dans les lignes qui suivent.

Il résulte de cette analyse que la proportion des hommes qui ont déclaré avoir été plus victimes de tentatives d'hameçonnage était 1,36 fois plus élevée que celle des femmes. Ce ratio baisse à 1,18 fois pour les victimes par infection virale. En revanche, les chiffres relatifs à la fraude sont presque similaires entre les hommes et les femmes, soit d'environ 4%.

L'analyse par groupes d'âge révèle que les internautes âgés de 75 ans et plus sont moins victimes que tous les autres groupes. Les écarts entre ce groupe et tous les autres sont assez significatifs pour que nous lui portions une attention particulière au paragraphe discussion.

Relativement à l'état civil du répondant, nous avons observé que les personnes divorcées ou séparées étaient de 1,6 à 2 fois plus susceptibles que les personnes mariées ou personnes vivant en union libre d'être victimes de fraude. En revanche, pour les autres sources de victimisation, cet écart est peu significatif.

En ce qui concerne le niveau de scolarité, la proportion d'internautes ayant le niveau collégial ou universitaire qui ont déclaré avoir été victimes de tentative d'hameçonnage était 1,4 fois plus élevée que les internautes qui n'avaient fait que des études primaires. Ces chiffres diffèrent quelque peu

[48] Risque attribuable à une caractéristique ou à un comportement.

de ceux trouvés par S. Perreault (Perreault, 2013) qui trouve que cette proportion est de deux entre les mêmes groupes.

Un autre facteur dont les résultats semblent surprenants est la langue. Les internautes anglophones qui ont déclaré avoir été victimes de tentative d'hameçonnage étaient 1,72 fois plus importants que les internautes d'expression française. En revanche, les anglophones qui ont déclaré être victimes de fraude étaient 1,2 fois plus élevés que les francophones.

Enfin, la proportion des internautes qui ont déclaré avoir été victimes de fraude en région métropolitaine est deux fois plus élevée que celle des personnes qui en ont été victimes en région éloignée (cf. tableau G.3). Cette proportion baisse respectivement à 1,3 et 1,1 pour les tentatives d'hameçonnage et les cas d'infection par un virus.

5.2.2 Caractéristiques liées au revenu et à l'emploi

L'analyse du critère de revenu annuel montre que parmi les internautes interrogés, les personnes dont le revenu annuel dépasse 100,000 $ sont environ 1,75 fois plus susceptibles que ceux qui en gagnent 20,000 $ et moins d'être victimes de tentative d'hameçonnage (cf. Tableau G.2). Ce ratio diminue à environ 1,2 fois pour les victimes d'infections et de fraude. On peut en déduire que le risque de victimisation a tendance à augmenter en fonction du revenu annuel.

Au sujet de l'impact de l'emploi sur la victimisation, les personnes en congé de maternité /paternité ou en maladie de longue durée étaient environ deux fois plus susceptibles d'être victimes de fraude que ceux dont l'activité principale était moins reposante (8,20 % par rapport à 4 %) (cf. tableau G.2). Ces résultats concordent à peu de chiffres près avec ceux de S. Perreault. (2013).

5.2.3 Caractéristiques liées à l'origine

Contrairement à l'article de Perreault (Perreault, 2013), notre étude analyse, entre autres critères qui caractérisent l'origine du participant, le fait d'être ou pas un autochtone. Le résultat d'analyse relatif à ce critère révèle que les autochtones avaient déclaré avoir été 1,41 fois plus à risque de victimisation par fraude que les non- autochtones. Ce ratio est un peu plus élevé chez les minorités visibles, soit de 1,9 fois plus que les non-minorités. Pour ce qui est des deux autres formes de victimisation, soit par infection ou par tentative réussie, les résultats diffèrent quelques peu (environ +/-10%) de ceux de S. Perreault (cf. tableau G.3). Ce qui nous fait dire que les autochtones

obtiennent, à quelques détails près, les mêmes scores que les immigrants reçus. En revanche, les minorités visibles sont légèrement plus à risque de victimisation par fraude que les autochtones et les immigrants.

5.2.4 Caractéristiques liées au comportement en ligne

> Le risque de fraude a tendance à s'accroitre, voire à doubler, en fonction de la fréquence d'utilisation d'Internet pour des transactions impliquant des renseignements personnels.

On constate, à la lecture du Tableau G.4, que 5,7% des internautes qui ont déclaré faire des réservations en ligne au moins une fois par jour ont été victimes de fraude. C'est 1,8 fois plus élevé que la proportion d'internautes qui ont rarement ou n'ont jamais fait des réservations en ligne. Cet écart passe à un peu plus du double lorsqu'il s'agit des opérations bancaires et des achats en ligne, c'est-à-dire que le risque de fraude a tendance à s'accroitre voire à doubler en fonction de la fréquence d'utilisation d'Internet pour des opérations en ligne qui requièrent forcément les renseignements bancaires. Ce qui n'est pas toujours le cas pour toutes les réservations.

On observe des écarts similaires pour les internautes qui ont déclaré avoir été victimes de tentatives d'hameçonnage. En revanche, l'écart se rétrécit (cf. Tableau G.4) dans le cas des infections et passe de l'ordre de 1,3 fois. C'est-à-dire que la proportion des internautes qui ont utilisé Internet pour faire des réservations, des achats et des opérations bancaires en ligne au moins une fois par jour est 1,3 fois plus élevée que la proportion des internautes qui ont rarement ou jamais fait ce type de transaction.

On peut en déduire que selon l'étude de l'ESG, l'utilisation fréquente d'Internet pour ce type de transaction semble accroitre significativement les risques de tentative d'hameçonnage et de fraude et un peu moins le risque d'infection. Toutes choses étant égales par ailleurs, l'influence sur le risque d'infection de l'utilisation d'Internet pour les transactions en ligne est comparable à celle de l'utilisation des réseaux sociaux et des salons de clavardage avec des ratios entre l'utilisation fréquente et la non-utilisation qui sont de l'ordre de 1,2 à 1,3. Nous reviendrons, au paragraphe intitulé *Discussion*, sur l'explication de ces résultats.

5.2.5 Caractéristiques liées aux contremesures de sécurité

> Les contremesures de sécurité prises par les internautes n'ont pas permis de réduire le risque de victimisation. Bien au contraire, elles semblent contribuer à l'augmenter.

La proportion des internautes victimes de fraude qui ont déclaré utiliser un antivirus est 1,3 fois plus élevée que ceux qui ont déclaré ne pas en utiliser (cf. Tableau G.5). On observe un écart similaire entre les internautes qui ont déclaré effectuer des transactions avec seulement des organisations biens connues et ceux qui ne font pas cette distinction. Ce ratio diminue à 1,15 lorsqu'il s'agit des internautes utilisant un pare-feu et de ceux qui ont déclaré utiliser des mots de passe forts et les changer de façon régulière. En outre, le risque de fraude semble augmenter lorsque l'internaute supprime régulièrement les fichiers temporaires. Ce résultat, à l'instar de celui sur l'impact de l'utilisation de l'antivirus et du pare-feu, est d'autant plus surprenant puisque ces contremesures font partie des mesures d'hygiène et de protection recommandées en sécurité informatique et l'application de telles mesures devrait plutôt réduire le risque et non l'augmenter. On retrouve la même surprise pour toutes les mesures contre les tentatives d'hameçonnage et les infections. Le risque semble donc augmenter chez les internautes ayant déclaré avoir utilisé un antivirus, un pare-feu, des mots de passe forts, etc. Nous y reviendrons au paragraphe *Discussion* pour tenter de comprendre ce paradoxe (P1[49]).

5.2.6 Classement des facteurs de risque individuel

Dans cette première analyse (tableau croisé) des réponses des internautes à l'enquête ESG 2009 sur la victimisation, nous venons d'établir des liens entre certaines variables catégorielles associées aux trois formes de victimisation que nous avons choisi d'étudier, notamment la tentative d'hameçonnage, les infections virales et la fraude par hameçonnage. Ces liens ont permis d'identifier les facteurs qui semblent, à des degrés divers, influencer le risque de victimisation. Par exemple, nous avons montré que la fréquence de certaines transactions en ligne (ex. opérations bancaires, réservations, achats), le revenu, le genre, le fait de résider dans une région urbaine, l'activité principale de l'internaute, sa fréquentation des réseaux sociaux et des sites de clavardage

[49]Paradoxe 1 : Les contremesures de sécurité prises par les internautes n'ont pas permis de réduire le risque de victimisation. Bien au contraire, elles semblent contribuer à l'augmenter.

augmenteraient le risque de tentative d'hameçonnage, toutes choses égales par ailleurs. Nous avons construit un tableau de classement de ces facteurs en fonction d'un ratio de proportion que nous avons défini comme étant la contribution au risque de chaque facteur. À titre d'exemple, la proportion des personnes qui ont déclaré faire des achats en ligne - au moins une fois par jour - est deux fois plus élevée que celles qui ont déclaré le faire rarement ou jamais. Dans ce cas, l'achat en ligne est un facteur de risque et le ratio de proportionnalité est de 2. Nous avons résumé tous ces facteurs ainsi que leur ratio de proportionnalité aux tableaux G.6, G.7 et G.8. En tout, ce sont 17 facteurs pour la tentative d'hameçonnage, 16 pour l'infection et 21 facteurs pour la fraude qui influent sur le risque de victimisation.

Le problème est que ces facteurs sont plus ou moins reliés les uns avec les autres. Par exemple, l'augmentation de la fréquence d'utilisation d'Internet pour des transactions en ligne peut être liée au fait que l'internaute soit en congé de maternité/paternité ou en maladie de longue durée et que lorsqu'il augmente la fréquence des transactions en ligne, il s'expose davantage à une tentative d'hameçonnage.

Face à un tel réseau de relations entre ces facteurs, on peut se demander comment faire la part de choses.

Est-ce que le sexe de l'internaute, son niveau de scolarité, son revenu ou encore sa fréquence d'utilisation d'Internet pour des transactions en ligne permettent de prédire la réussite ou l'échec d'une des formes de victimisation étudiée dans ce travail ?

L'analyse que nous avons faite jusqu'ici ne permet pas de répondre à cette question. Ce que nous envisageons de faire pour expliquer l'importance de la variation de la tentative d'hameçonnage (ou de l'infection voire de la fraude) à partir de tous ces facteurs, c'est de développer un modèle de régression logistique binaire qui nous permettra de prédire le plus efficacement possible chacune des formes de victimisation ci-dessus.

Notre hypothèse est qu'il y a au moins un des facteurs du modèle qui est associé significativement à la réussite ou à l'échec de la tentative d'hameçonnage, de l'infection ou de la fraude par hameçonnage.

5.3 Analyse des facteurs de risque multiple

5.3.1 Modèle d'analyse de régression logistique binaire

Notre modèle cherche à expliquer la survenue d'un des trois évènements (ou formes) de victimisation par hameçonnage suivants :

- e_1 pour tentative d'hameçonnage
- e_2 pour infection et
- e_3 pour fraude

Notons Y_i la variable dépendante binaire associée à l'évènement *i*.

$$Y_i = \begin{cases} 1, \text{si occurrence de l'évènement} \\ 0, \quad \text{en cas de non occurrence} \end{cases}$$

- Avec i ∈ {e_1, e_2, e_3}

La probabilité d'occurrence de l'événement *i* (odds ou cote en français) est définie comme la probabilité qu'il arrive divisée par celle qu'il n'arrive pas et peut être représentée par l'équation :

$$odds = \frac{p}{1-p} = e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n} \text{ et donc } p = \frac{e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n}}{1+e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n}},$$

où $x_1, x_2, \ldots . x_n$ sont les variables indépendantes. Ces variables représentent les facteurs de risque que nous avons identifiés au paragraphe précédent comme étant susceptibles d'influencer la survenue de l'une ou de l'autre des formes de victimisation à l'étude dans ce travail (cf. tableaux G.6, G.7 et G.8). Parmi ces variables, certaines sont catégorielles, (comme le genre ou encore le nombre de fois que l'internaute a utilisé Internet pour effectuer des opérations bancaires électroniques). Dans ce cas, nous les remplaçons dans l'équation par des variables dichotomiques.

Par exemple, dans le cas ci-dessous, la variable IRP_Q115[50] prend 5 modalités (1[51],2[52], 3[53], 4[54], 5[55]) dont la dernière modalité (5) est considérée comme le groupe de référence auquel les autres sont comparés. La variable IRP_Q115 sera donc représentée par quatre variables dichotomiques, x_1, x_2, x_3, x_4, x_5 étant toujours égale à 1.

Le rapport de deux cotes peut être calculé de la manière suivante :

$$si\ x_1 = 1, \qquad \frac{p}{1-p} = e^{\beta_0+\beta_1+\beta_2 x_2+\cdots+\beta_n x_n} \text{ et } si\ x_1 = 0, \frac{p}{1-p} = e^{\beta_0+0+\beta_2 x_2+\cdots+\beta_n x_n}$$

Ce rapport entre ces deux cotes est donc de :

$$\frac{e^{\beta_0+\beta_1+\beta_2 x_2+\cdots+\beta_n x_n}}{e^{\beta_0+0+\beta_2 x_2+\cdots+\beta_n x_n}} = e^{\beta_1}$$

Donc e^{β_1} est le rapport des cotes et noté «Exp(B)» dans le tableau H1. C'est l'accroissement relatif –risque relatif- dû à une augmentation d'une unité de la variable indépendante. Lorsque ce ratio est plus grand que 1, la probabilité augmente avec le changement.

$\beta_1 > 0 \Rightarrow e^{\beta_1} > 1 \Rightarrow$ les odds sont supérieures si $x_1 = 1$.

Si x_1 est quantitatif , l'accroissement relatif des odds si x_1 croît d'une quantité d, est

$$\frac{e^{\beta_0+\beta_1(x_1+d)+\beta_2 x_2+\cdots+\beta_n x_n}}{e^{\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n}} = e^{\beta_1 d}$$

---

[50] Au cours du dernier mois, combien de fois avez-vous utilisé Internet pour effectuer des opérations bancaires électroniques ?

[51] Au moins une fois par jour

[52] Au moins une fois par semaine

[53] Au moins une fois par mois

[54] Pas au cours du dernier mois ou jamais

[55] Ne possède pas de compte bancaire

Donc en prenant d =1, e^{β_1} représente l'accroissement relatif des odds pour un accroissement d'une unité de x_1.

Cet accroissement saisit la contribution du groupe x_1 au risque de victimisation par rapport à un groupe de référence. Lorsqu'il est statistiquement significatif et supérieur à 1, il indique que la variable en question accroît le risque de victimisation. En revanche, lorsqu'il est statistiquement significatif et inférieur à 1, il indique que la caractéristique en question réduit le risque de victimisation.

5.3.2 Résultats d'analyse de régression logistique

Au paragraphe 4.1.6 nous avons confirmé l'hypothèse de dépendance entre un certain nombre de facteurs et les variables dépendantes associées à l'une ou l'autre des trois formes de victimisation par hameçonnage étudiées dans cette recherche. Ce que nous tentons de faire maintenant, c'est d'analyser les mêmes facteurs en appliquant notre modèle de régression dans l'optique de valider si ces facteurs permettraient de prédire une de ces formes de victimisation.

Pour valider notre modèle, nous reprenons les caractéristiques liées au comportement en ligne. Les trois variables y afférentes sont catégorielles. Nous pouvons donc identifier pour chacune d'elle le groupe de référence à partir duquel comparer les autres groupes. Ainsi, ces trois variables IRP_Q115, IRP_Q1130 et IRP_Q135, ont le même groupe de référence, c'est-à-dire, ceux qui ont déclaré qu'ils *«…ne se servent jamais d'Internet pour des opérations bancaires ou faire des réservations ou encore faire des achats en ligne»* pour l'une ou l'autre des transactions susmentionnées.

Les résultats d'analyse montrent que la fréquence d'utilisation d'Internet pour des opérations bancaires en ligne contribue à accroitre le risque de tentative d'hameçonnage. En effet, le rapport de cotes du groupe ayant déclaré utiliser Internet au moins une fois par mois pour effectuer les opérations bancaires est 1,35 fois supérieur à celui des internautes qui n'utilisent jamais Internet pour effectuer les opérations bancaires et celui des internautes qui utilisent Internet au moins une fois par jour est 1,5 fois supérieur à celui du groupe de référence (cf. tableau H1). Pour la variable associée à la fréquence d'utilisation d'Internet pour des réservations en ligne (IRP_Q130), les résultats sont très similaires à ceux que nous venons de présenter. En revanche, le rapport de cotes

augmente à 2,44 fois lorsqu'on compare les internautes qui utilisent Internet au moins une fois par jour pour des achats en ligne au groupe de référence.

Dans le cas d'une infection par hameçonnage, les résultats obtenus sur l'utilisation d'Internet pour effectuer des opérations bancaires et les réservations en ligne ne sont pas statistiquement significatifs puisque p[56]>0,05 (p=0,106 pour IRP_Q115 et p=0,102 pour IRP_Q130) comme on peut l'observer dans le tableau H.2. Par contre, le fait d'utiliser Internet pour faire des achats des produits et services augmente la probabilité d'infection (p=000 pour IRP_Q135).

Enfin, pour la fraude, la fréquence d'utilisation d'Internet pour les opérations bancaires et achats en ligne augmente la probabilité d'être victime (cf. rapport de cotes tableau H.3).

À la lumière de ces résultats, on peut conclure que :

- R_1 *: plus la fréquence d'utilisation d'Internet pour effectuer les opérations bancaires et les achats en ligne est élevée, plus grand est le risque d'être victime de tentative d'hameçonnage et de fraude.*

Nous reviendrons au paragraphe *Discussion* pour expliquer ce résultat, mais pour la suite, les résultats d'analyse des caractéristiques sociodémographiques révèlent que :

1. Comparativement aux femmes (qui est le groupe de référence), les hommes présentent un risque 1,6 fois plus élevé d'être victime de tentative d'hameçonnage ou d'infection (cf. rapport de cotes, Tableau H.1 et H.2).
2. Les internautes qui parlent anglais seulement ont un risque 1,3 fois supérieur d'être victimes de tentative d'hameçonnage à ceux qui ont déclaré qu'ils parlaient une autre langue [Exp(B) = 1,32]. À l'inverse, on observe chez les internautes qui parlent francais une diminution du risque par rapport à ceux qui parlent une autre langue [Exp(B) = 0,63]. Des explications suivront au paragraphe discussion.
3. La relation entre le niveau de scolarité et le risque d'infection est négative (ex. Exp(B) = 0,49 pour le niveau primaire par rapport au groupe de référence qu'est le niveau universitaire avec Exp(B) = 0,88 (cf. tableau H.2), c'est donc dire que ceux qui ont le niveau

[56] Pour *p*-value. C'est la valeur qui, si elle est inférieure à un certain seuil (conventionnellement fixé à 5 %) permet de déclarer que la relation est significative. Plus la valeur est faible, plus sécuritaire est notre conclusion.

de scolarité primaire ont une plus faible probabilité que les universitaires d'être victimes d'infection. Quant à la relation entre le risque de tentative d'hameçonnage et le niveau de scolarité, elle est globalement négative (cf. tableau H.1). Ce que nous attribuons au hasard. On en conclut globalement que plus le niveau de scolarité est élevé, plus grandes sont les chances d'être victime de tentative d'hameçonnage.

- R_2 *: Les hommes sont plus susceptibles que les femmes d'être victimes de tentative d'hameçonnage ou d'infection.*
- R_3 *: Le niveau de scolarité augmente le risque de victimisation par tentative d'hameçonnage ou d'infection.*
- R_4 *: Les internautes dont la langue de ménage est l'anglais sont plus susceptibles que ceux qui ont déclaré parler le francais ou autre langue d'être victime de tentatives d'hameçonnage et d'infection. A contrario, le fait de parler français diminue le risque d'être victime de tentative d'hameçonnage.*

Quant à l'analyse des caractéristiques liées au revenu, nous obtenons le résultat suivant :

1. La relation entre le revenu et le risque de fraude est négative [Exp(B) = 0,52], c'est donc dire que les internautes qui avaient un revenu faible, inférieur 39999 $, avaient une plus faible probabilité que ceux qui étaient riches (revenu supérieur 80000 $) d'être victime de fraude. Il en est de même pour la relation entre revenu et tentative d'hameçonnage (Exp(B) = 0,72). Par contre, dans le cas de la victimisation par infection, nos résultats ne sont pas statistiquement significatifs.
2. R_5 *: Les riches sont plus susceptibles d'être victimes de tentative d'hameçonnage et de fraude que les pauvres.*
3. Le risque d'être victime d'infection par hameçonnage augmente si l'internaute utilise un antivirus pour assurer sa sécurité sur Internet. En effet, les internautes qui ont déclaré avoir été victimes d'infection alors qu'ils avaient un antivirus sur leur ordinateur étaient 2,5 fois plus élevés que ceux qui ont été victimes mais qui n'avaient pas d'antivirus sur leur machine. Ce résultat est contre-intuitif voire paradoxal car un antivirus est une contremesure qui est censée protéger l'internaute contre les menaces. Or, c'est l'effet inverse qui semble s'être produit.
4. Changer régulièrement les mots de passe, utiliser un pare-feu, supprimer régulièrement les fichiers temporaires ou encore supprimer régulièrement les courriels d'expéditeurs inconnus augmentent la probabilité d'être victime de tentative d'hameçonnage (cf. rapport

de cotes au tableau H.1). En revanche, les résultats obtenus dans le cas de victimisation par fraude ne sont pas statistiquement significatifs ($p > 0,05$). On ne peut donc conclure à un effet de ces contremesures sur cette forme de victimisation.

5. Supprimer régulièrement les fichiers Internet temporaires augmente la probabilité de se faire infecter (c.f Exp(B) = 1,29 au tableau H.2).
6. Les résultats obtenus pour les internautes qui ont déclaré traiter seulement avec les organisations bien connues ne sont pas statistiquement significatifs pour les trois formes de victimisation.

Les résultats obtenus en (5), (6) et (7) confirment l'évidence du paradoxe P1 :

P1: *les contremesures de sécurité prises par les internautes n'ont pas permis de réduire le risque de victimisation. Bien au contraire, elles semblent contribuer à l'augmenter.*

Nous y reviendrons au paragraphe intitulé *Discussion*.

Pour ce qui est des autres caractéristiques, nos résultats révèlent ce qui suit :

1. Le fait d'appartenir à un groupe de réseautage social ou d'avoir utilisé Internet pour se connecter à un salon de clavardage est un facteur qui augmente la probabilité d'être victime de tentative d'hameçonnage (cf. rapport de cotes Exp(B) = 1,28 Exp(B) = 1,56 au tableau H.1) ou de se faire infecter (cf. rapport de cotes Exp(B) = 1,19 Exp(B) = 1,76 au tableau H.2). En revanche, ces deux variables ne semblent pas avoir un effet sur la fraude car le rapport de cote est plus ou moins égal à 1 (Exp(B) = 1,036 et Exp(B) =1,042).
2. L'internaute qui vit en région urbaine est plus susceptible d'être victime de tentative d'hameçonnage ou d'infection que celui qui vit en région rurale (cf. Exp(B) =1,27, p=000, Tableau H.1 ; Exp(B) =1,17, p=0,003, au tableau H.2).
3. L'activité principale de l'internaute semble avoir un effet sur une seule forme de victimisation : l'infection. Pour les deux autres formes de victimisations, nos résultats sont statistiquement non significatifs.
4. Le fait de prendre des mesures accrues ne réduit pas le risque de victimisation par tentative d'hameçonnage. Le Tableau H.5 résume les résultats de l'analyse des liens entre la victimisation et le nombre de contremesures prises par l'internaute. On y observe que la

proportion des internautes qui ont déclaré avoir été victimes de tentative d'hameçonnage croit légèrement à mesure que le nombre de contremesures déclarées augmente. Par exemple, 72,1% des internautes qui ont déclaré avoir un antivirus et un pare-feu ont été victime de tentative d'hameçonnage. Ce chiffre passe à 72,4% puis à 77,2% et enfin à 79,6% lorsque les internautes déclarent disposer respectivement de 3, 4 et 5 contremesures. Les autres résultats d'analyse de liens probables entre l'augmentation du nombre de contremesures et la victimisation par infection ou par fraude ne suivent aucune logique univoque sur laquelle nous pouvons tirer une quelconque conclusion.

Avant de poursuivre avec le résumé des résultats de notre analyse, rappelons que l'objectif de notre modèle de régression est d'expliquer l'importance de la variation de la tentative d'hameçonnage, de l'infection et de la fraude à partir des facteurs que nous avons identifiés avec les tableaux croisés. En d'autres termes, tenter de prédire chacune de ces formes de victimisation. L'analyse de régression logistique effectuée permet d'identifier un certain nombre de facteurs prédicteurs de victimisation. Nous les résumons comme suit :

- R_1 : La fréquence d'utilisation d'Internet pour effectuer les opérations bancaires et les achats en ligne est un important facteur de prédiction de la tentative d'hameçonnage et de la fraude.
- R_2 : Les hommes sont plus susceptibles que les femmes d'être victimes de tentative d'hameçonnage ou d'infection.
- R_3 : Le niveau de scolarité augmente le risque de victimisation par tentative d'hameçonnage ou par infection.
- R_4 : Les internautes dont la langue de ménage est l'anglais sont plus susceptibles que ceux qui ont déclaré parler le français ou une autre langue d'être victime de tentatives d'hameçonnage et d'infection. À contrario, le fait de parler français diminue le risque d'être victime de tentative d'hameçonnage.
- R_5 : Les riches sont plus susceptibles d'être victimes de tentative d'hameçonnage et de fraude que les pauvres.

R_6 : La fréquentation des sites de réseautage social et l'utilisation du service de clavardage augmente le risque de victimisation par tentative d'hameçonnage ou par infection.

R_7 : L'internaute qui vit en région urbaine est plus susceptible d'être victime de tentative d'hameçonnage ou d'infection que celui qui vit en région rurale.

R_8 : L'activité principale de l'internaute semble avoir un effet sur une seule forme de victimisation : l'infection. Pour les deux autres formes de victimisations, nos résultats sont statistiquement non significatifs.

R_9 : Le fait de prendre des mesures accrues ne réduit pas le risque de victimisation par tentative d'hameçonnage.

Aussi, notre analyse de régression révèle un paradoxe important relatif aux contremesures de sécurité. Nous l'énonçons comme suit :

P1 : Les contremesures de sécurité prises par les internautes n'ont pas permis de réduire le risque de victimisation. Bien au contraire, elles semblent contribuer à l'augmenter.

Il est intéressant de souligner que ce paradoxe est le même que celui que nous avons formulé après l'analyse par des tableaux croisés et que S. Perrault (2011) a aussi énoncé dans son article.

Plusieurs raisons peuvent expliquer ce paradoxe. Tout d'abord, on est en droit de se demander si les participants interrogés avaient mis en place les contremesures en question seulement après avoir été victimes de tentative d'hameçonnage ou d'infection ! Si c'est le cas, les contradictions qui résultent de leurs réponses seraient justifiées. Malheureusement, le rapport d'enquête de l'ESG ne mentionne pas cette information. Toutefois, il nous semble étrange qu'un si grand nombre de répondants ait pris les mesures de protections seulement après avoir été victime.

Si ce n'est pas le cas, il est possible que des internautes qui croient être protégés, du fait qu'ils ont pris des contremesures, adoptent des comportements très risqués. Ce qui ressemblerait alors à un effet pervers qu'on qualifie dans certaines situations de risque moral.

Notre démarche de recherche étant exploratoire, la réflexion autour de la ou des raisons qui expliquent ce paradoxe (P1) soulève une sous-question de recherche qui n'a pas été considérée au départ et que nous adressons dans les lignes qui suivent.

En fait, ce que nous voulons savoir c'est :

> est-ce que le fait d'avoir pris des contremesures de sécurité est un incitatif à la prise de risque ?

Pour répondre à cette question, nous analysons au paragraphe qui suit le lien potentiel entre le niveau de protection que les internautes déclarent avoir pris (via le nombre de contremesures) et l'adoption de certains comportements à risque. Pour cela, nous utilisons le concept d'Aléa moral pour faire cette analyse.

5.3.3 Risque moral

C'est un concept qui a été utilisé de diverses façons par différentes disciplines depuis plus de 200 ans (Dembe & Boden, 2000). La littérature révèle qu'il existe plusieurs définitions de ce concept selon le domaine dans lequel il est appliqué. Mais en dépit des nuances contextuelles, l'examen de ces définitions révèle qu'elles se ressemblent et se recoupent. La définition qui suit, proposée par Allard E. Dembe et al., est conforme à l'utilisation que nous souhaitons en faire pour cette discussion.

> «Le risque moral est la tendance des régimes d'assurance à encourager un comportement qui augmente le risque de perte assurée» (Dembe & Boden, 2000).

L'exemple que nous avons trouvé dans la littérature pour appuyer cette définition du risque moral a été proposé par Douglass dans son article intitulé «An examination of the fraud liability shift in consumer card-based payment systems». Il dit ceci :

> «Si un participant à un système de paiement donné n'a aucun risque de perte en raison des transactions frauduleuses, ce participant peut avoir peu d'incitation à prendre des mesures, même de la nature la plus simple, pour éviter ou réduire la probabilité de fraude». Traduction de (Douglass, 2009).

Dans ce travail de recherche, nous définissons le risque moral comme étant :

> «La perspective qu'un internaute, supposément isolé d'un des risques de victimisation par hameçonnage, se comporte différemment que s'il y était totalement exposé».

Supposément isolé du risque veut dire que l'internaute a répondu «Oui» à l'une des questions suivantes :

a) Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?
b) Pour protéger votre sécurité sur Internet : ... utilisez-vous un pare-feu?
c) Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?
d) Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?
e) Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les fichiers Internet temporaires?

Se comporter différemment veut dire que l'internaute a répondu par un, deux, ou trois à chacune des trois questions inhérentes aux transactions en ligne et par «Oui» aux deux questions qui portent sur la socialisation en ligne.

- 1 signifie qu'il utilise Internet «au moins une fois par jour»
- 2 signifie qu'il utilise Internet «au moins une fois par semaine»
- 3 signifie utilise Internet «au moins une fois par mois».

Les trois questions liées aux transactions en ligne :

a) Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?
b) Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?
c) Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?

Les deux questions liées à la socialisation en ligne :

i. Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace?
ii. Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?

5.3.4 Résultats de l'analyse du risque moral

Le tableau de contingence (cf. Tableau H.4) nous apprend que 77,7 % des 237 internautes qui ont déclaré avoir un antivirus et un pare-feu ont effectué des opérations bancaires. Cette proportion est de 80% lorsque l'internaute prend une ou deux autres contremesures additionnelles comme la suppression des courriels des expéditeurs inconnus ou encore le fait de supprimer régulièrement les fichiers temporaires. En revanche, elle baisse un tout petit peu lorsque la contremesure consiste à changer régulièrement les mots de passe. On observe un phénomène un peu similaire chez les internautes qui ont déclaré avoir acheté les produits et services. Par contre, chez les internautes qui ont déclaré avoir fait des réservations en ligne ou ceux qui fréquentent des salons de clavardage, cette proportion croit invariablement avec le nombre de contremesures. Par exemple, pour l'antivirus et le pare-feu, elle est de 42,6%. Si, en plus l'internaute supprime les courriels des expéditeurs inconnus et change régulièrement ses mots de passe, la proportion passe à 48,5%. Elle atteint les 49,5% lorsque l'internaute déclare avoir déployé toutes les cinq contremesures. Enfin, pour les internautes qui ont déclaré appartenir à un réseau social, le fait de prendre des mesures accrues ne semble pas avoir impacté la manière de socialiser en ligne. Nous reviendrons sur ces résultats au paragraphe consacré à la discussion.

5.4 Discussion

L'application de notre modèle de régression aux données de l'ESG confirme, à la fois, les résultats obtenus dans notre première analyse (tableaux croisés) et, en partie, les résultats des travaux de S. Perreault (2011) à l'effet qu'il existe des relations significatives entre certains facteurs sociodémographiques et les trois formes de victimisation étudiées dans ce travail de recherche. Nos résultats indiquent que :

C_1: être un homme, être plus scolarisé, être riche, vivre en milieu urbain augmentent les probabilités d'être victime de tentative d'hameçonnage;

C_2: être un homme, être plus scolarisé, parler anglais, vivre en milieu urbain augmentent les probabilités de se faire infecter. De plus, l'activité principale de l'internaute semble avoir un effet sur le fait de se faire infecter.

C_3: être riche augmente les probabilités d'être victime de fraude.

Être un homme augmente le risque d'être victime de tentative d'hameçonnage et d'infection

La littérature consultée sur la question est partagée, certains travaux concluent que les femmes sont plus susceptibles que les hommes d'être victimes de tentative d'hameçonnage (Abraham, Morn, & Vollman, 2010; Darwish, El Zarka, & Aloul, 2012; Kumaraguru et al., 2010; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) et d'infection. Pour d'autres, il n'y a pas de différence significative entre les hommes et les femmes (Lalonde Levesque, Nsiempba, Fernandez, Chiasson, & Somayaji, 2013) alors qu'une troisième catégorie trouve qu'être un homme augmente le risque de tentative d'hameçonnage et d'infection. Nos résultats s'inscrivent dans cette troisième perspective. Toutefois, en poussant la réflexion plus loin, on arrive à l'idée que ce n'est peut-être pas tant le genre qui influence la victimisation mais les prédicteurs comme la sensibilisation aux enjeux de sécurité ou le profil de risque de l'individu. Or, les données de l'enquête ESG ne permettent pas d'étudier ces deux prédicteurs. En revanche, le chapitre 6 aborde un tout petit peu la question en examinant le profil de risque du fraudeur dans le processus de monétisation des renseignements volés par hameçonnage.

Être scolarisé augmente le risque d'être victime de tentative d'hameçonnage et d'infection

Nos analyses confirment ainsi le lien entre niveau de scolarité et la victimisation par tentative d'hameçonnage et par infection. Plusieurs auteurs (Graham & Triplett, 2016), avant nous, ont étudié ce lien et ont tiré la même conclusion que nous. Toutefois, aucune de ces études n'a été faite sur un échantillon aussi grand que celui de l'enquête ESG. Nos résultats viennent donc confirmer et renforcer cette thèse.

Être riche augmente le risque d'être victime de tentative d'hameçonnage et de fraude

Le rapport de la firme Gartner (Raisbeck, November 10, 2006) montre que les cybercriminels ciblent davantage les personnes riches, c'est-à-dire des cibles intéressantes. Être une cible intéressante suppose que l'internaute adopte des comportements qui laissent croire à l'attaquant qu'il possède des biens qui peuvent l'intéresser. Par exemple, le fait de fréquenter les plates-formes partagées par un certain nombre de banques, des systèmes de paiement (ex. Boleto, Bitcoin) et les entreprises qui gèrent les renseignements personnels. Nos résultats d'analyse de tableau croisé et de régression logistique avec les données de l'enquête ESG confirment les conclusions de Gartner en ce sens que les internautes dont les revenus dépassaient 80000 $ (Dupont, 2013) ont enregistré une probabilité plus élevée d'être victime de tentative d'hameçonnage et de fraude.

Vivre en milieu urbain augmente le risque d'être victime de tentative d'hameçonnage et d'infection

Pour bien comprendre ce résultat, nous devons examiner la différence dans la fréquence d'utilisation d'Internet entre les régions rurales et les régions urbaines. 65,2% des personnes qui ont déclaré avoir utilisé Internet au cours des 12 derniers mois provenaient des régions urbaines contre seulement 32,8% qui résidaient en région rurale. Cela pourrait résulter des effets structurels liés à la faible accessibilité à Internet de la maison ou des lieux publics en région rurale dans les années 2008-2009. Nos résultats sont donc en phase avec ceux de S. Perreault.

Parler anglais augmente le risque d'être victime de tentative d'hameçonnage et d'infection

Nos résultats indiquent que les internautes dont la langue de ménage est l'anglais sont plus susceptibles d'être victimes de tentatives d'hameçonnage et d'infection que ceux qui ont déclaré parler le français ou autre langue. À contrario, le fait de parler français diminue le risque d'être victime de tentative d'hameçonnage. Cette tendance pourrait s'expliquer, selon Perreault (Perreault & Brennan, 2010), par l'effet protecteur qu'offre la langue française dans le cyberespace. Une analyse de la victimisation de la population québécoise effectuée par l'Institut de la Statistique du Québec abonde dans le même sens. Ce résultat serait encore plus intéressant si on est à mesure d'identifier les éléments de protections sous-jacents afin de déterminer avec plus de certitude si c'est vraiment la langue en tant que telle ou à l'attitude prudente voire attentive du francophone face à une langue étrangère qui contribue à augmenter le risque. Une telle attitude qui l'astreint à examiner en détails les messages qu'il reçoit.

Relativement aux caractéristiques liées au comportement en ligne, les résultats de nos analyses révèlent que :

C_4 : la fréquence d'utilisation d'Internet pour effectuer les opérations bancaires et les achats en ligne est un important facteur de prédiction de la tentative d'hameçonnage et de la fraude.

Ce résultat valide en partie nos hypothèses H4.1.a, H4.2.a et H4.4.a. Nous disons en partie parce que le fait d'utiliser Internet pour faire des réservations ne semble pas avoir un effet sur la victimisation quelle qu'en soit le type. L'explication la plus plausible a été donnée au paragraphe 4.2.4. Nous y avons soutenu que le risque de fraude est plus élevé lorsque les transactions en ligne

requièrent inévitablement les renseignements bancaires comme les opérations bancaires et les achats en ligne. Ce qui n'est pas toujours le cas pour toutes les réservations.

C_5 : La fréquentation des sites de réseautage social et l'utilisation des salons de clavardage augmentent le risque de victimisation par tentative d'hameçonnage ou par infection.

Nos résultats concordent avec ceux de S. Perreault (Perreault) sur ces deux formes de victimisation tout en différant sur la troisième forme. En effet, nous n'avons pas trouvé de lien entre le fait de fréquenter les réseaux sociaux et les salons de clavardage et la victimisation par fraude telle que nous l'avons définie plus haut dans ce travail. En conclusion, les résultats de notre recherche valident nos hypothèses H4.1.b pour la victimisation par tentative d'hameçonnage et H4.2.b pour la victimisation par infection et, invalide l'hypothèse H4.4b relative à la victimisation par fraude. Encore une fois, le risque de fraude semble être lié à la nature des renseignements que l'internaute échange en ligne. Or, la fréquentation des réseaux sociaux et des salons de clavardage ne requiert pas l'utilisation de tels renseignements sensibles.

Avant de présenter notre prochaine conclusion, rappelons qu'à l'issue de nos analyses de régression et de tableaux croisés, les résultats d'analyse de la relation entre les contremesures et la victimisation ont révélé que «les contremesures de sécurité prises par les internautes n'ont pas permis de réduire le risque de victimisation. Bien au contraire, elles semblent contribuer à l'augmenter» P1. Nous avons voulu savoir si ce paradoxe était valide lorsque l'internaute prend plus d'une contremesure (mesures accrues) pour se protéger. Le résultat d'analyse indique que :

C_6 : Le fait de prendre des contremesures n'a pas réduit le risque de victimisation par tentative d'hameçonnage.

Le paradoxe P1 se confirme également lorsque l'internaute déclare avoir pris plusieurs contremesures de sécurité pour sa protection en ligne.

L'analyse de ce paradoxe nous a conduit en cours de recherche à poser la sous question de recherche suivante : *Est-ce que le fait d'avoir pris des contremesures de sécurité est un incitatif à la prise de risque ?*

Pour répondre à cette question, nous avons effectué une analyse des liens potentiels entre le fait d'avoir pris des contremesures et l'adoption des comportements à risque (analyse du risque Moral).

Si l'on exclut les internautes qui ont déclaré appartenir à un réseau social, les résultats obtenus semblent globalement suggérer que plus le nombre de contremesures de protection déclarées augmente, plus la fréquence d'utilisation d'Internet pour effectuer des transactions en ligne et pour fréquenter les salons de clavardage est élevée. Nos résultats d'analyse indiquent donc qu'il semble y avoir un lien probable entre le fait d'avoir pris des contremesures et l'adoption, par l'internaute, de comportements susceptibles d'augmenter le risque de victimisation par tentative d'hameçonnage et par infection. Une telle attitude s'apparente à ce que N. Luhmann appelle la confiance assurée (Luhmann, 2001). C'est-à-dire que l'internaute est assuré que les contremesures qu'il a prises contre les risques de victimisation lui garantissent un niveau de sécurité élevé, lequel niveau de sécurité devient une espèce d'incitatif à la prise de risque. L'internaute ne semble pas alors tenir compte de la survenue d'évènements contingents. Au contraire, il augmente sa fréquence d'utilisation d'Internet au risque de se faire prendre.

Cette conclusion sur l'utilisation du concept d'Aléa moral pour expliquer la prise de risque des utilisateurs qui ont déclaré avoir pris des contremesures pour se protéger ressemblent à deux situations que nous avons recensées dans la littérature. Anderson et al. relatent, qu'en Grande Bretagne, dans les années 80, les banquiers britanniques avaient une telle confiance en la sécurité de leur système de guichet automatique (ATM) que lorsqu'un client contestait une transaction, c'était soit qu'il était menteur, soit qu'il s'était trompé. Résultat, les banquiers se sont retrouvés avec un système de sécurité plus cher et avec plus de cas de fraudes sur la main (Anderson & Moore, 2006).

L'autre exemple n'est pas tout à fait pareil, mais s'en approche. Dans une étude clinique sur les infections en sécurité informatique, F. Lalonde et al. affirment que les utilisateurs ayant un niveau d'expertise élevé en informatique présentent un risque plus élevé d'infection (Lévesque, Davis, & Fernandez).

Un bémol est toutefois à faire dans l'application de ce concept dans notre recherche. Les écarts entre les mesures d'associations de ces variables ne sont pas élevés. À la lumière donc de ce bémol, nos résultats ne sont pas suffisamment convaincants pour que l'on en tire une conjecture précise. Nous suggérons qu'une étude spécifique soit menée avec des données précises sur le sujet.

Tableau 5.1 : Sommaire des facteurs de prédiction de victimisation - Formes de victimisation

Facteurs	Par tentative d'hameçonnage	Par infection	Par fraude
Facteurs de prédiction	1. Fréquence d'utilisation d'Internet pour les achats et opérations bancaires en ligne		1. Fréquence d'utilisation d'Internet pour les achats et opérations bancaires en ligne
	2. Vivre en région urbaine 3. Être un homme 4. Être scolarisé 5. Parler anglais 6. Fréquenter les réseaux sociaux et les salons de clavardage	1. Vivre en région urbaine 2. Être un homme 3. Être scolarisé 4. Parler anglais 5. Fréquenter les réseaux sociaux et les salons de clavardage	
	7. Être riche		2. Être riche
		6. Type d'activité principale	
Éléments à approfondir	Efficacité des contremesures Risque moral	Efficacité des contremesures Risque moral	Signalement à temps des incidents auprès des banques Mesures additionnelles de protection des comptes (assurances protection)

5.5 Conclusion

Rappelons que l'objectif de ce chapitre était double : analyser les facteurs qui contribuent à la victimisation par hameçonnage et les classer par ordre de priorité. Et, utiliser la notion d'Aléa moral pour étudier les comportements des internautes face au risque de victimisation. Un pari difficile à atteindre et nous en étions parfaitement conscients.

À la lumière de toutes les analyses que nous avons effectuées sur les données de l'enquête ESG 2009 de Statistique Canada, nos résultats permettent de se rapprocher de ces objectifs. En effet, nous avons trouvé que la fréquence d'utilisation d'Internet pour effectuer les achats et les opérations bancaires en ligne est plus prédictible de tentative d'hameçonnage et de fraude que tous

les autres facteurs de risque. Pour la victimisation par infection, le facteur de prédiction le plus important est l'utilisation des salons de clavardage suivie, étonnamment, du genre et de l'activité principale de l'internaute. Les autres facteurs de prédictions sont résumés, par ordre d'importance, dans le tableau 5.1 ci-dessus.

On y observe, dans la dernière ligne, des facteurs potentiels comme l'efficacité des contremesures, le risque moral ou encore le signalement à temps des incidents. Ces facteurs ne peuvent être retenus dans cette recherche que comme pistes de réflexion et d'étude car des données précises sont à colliger et, sans celles-ci, nous ne pouvons tirer de conclusion.

On y remarque aussi, dans la colonne de droite, que la fraude n'a que deux facteurs de prédiction : la fréquence d'utilisation d'Internet pour les achats et les opérations bancaires en ligne et le fait d'être riche. Deux facteurs qui, en réalité n'en font qu'un : adopter des comportements qui fassent de l'internaute une cible intéressante. Or, nous avons défini la fraude, au début de ce chapitre, comme étant le retrait de l'argent du compte de la victime, c'est-à-dire l'aboutissement du processus de monétisation. Ce n'est donc pas une coïncidence si l'analyse des données de l'enquête ESG 2009 donne ce faible nombre de facteurs de risque de fraude. En fait, aucune variable dans ce sondage ne permet de colliger les informations sur le processus de monétisation. Et, c'est pour cette raison- *manque de données sur le marché noir des renseignements volés*- que nous avons choisi de proposer un modèle théorique de ce phénomène et, c'est d'ailleurs l'objet du chapitre 6 qui suit.

Le second bloc de l'approche de réduction de risque que nous proposons dans cette thèse est ainsi partiellement complété. Il s'agit des facteurs de prédiction de risque d'hameçonnage bancaire

(cf. Figure 5.1 ci-dessous).

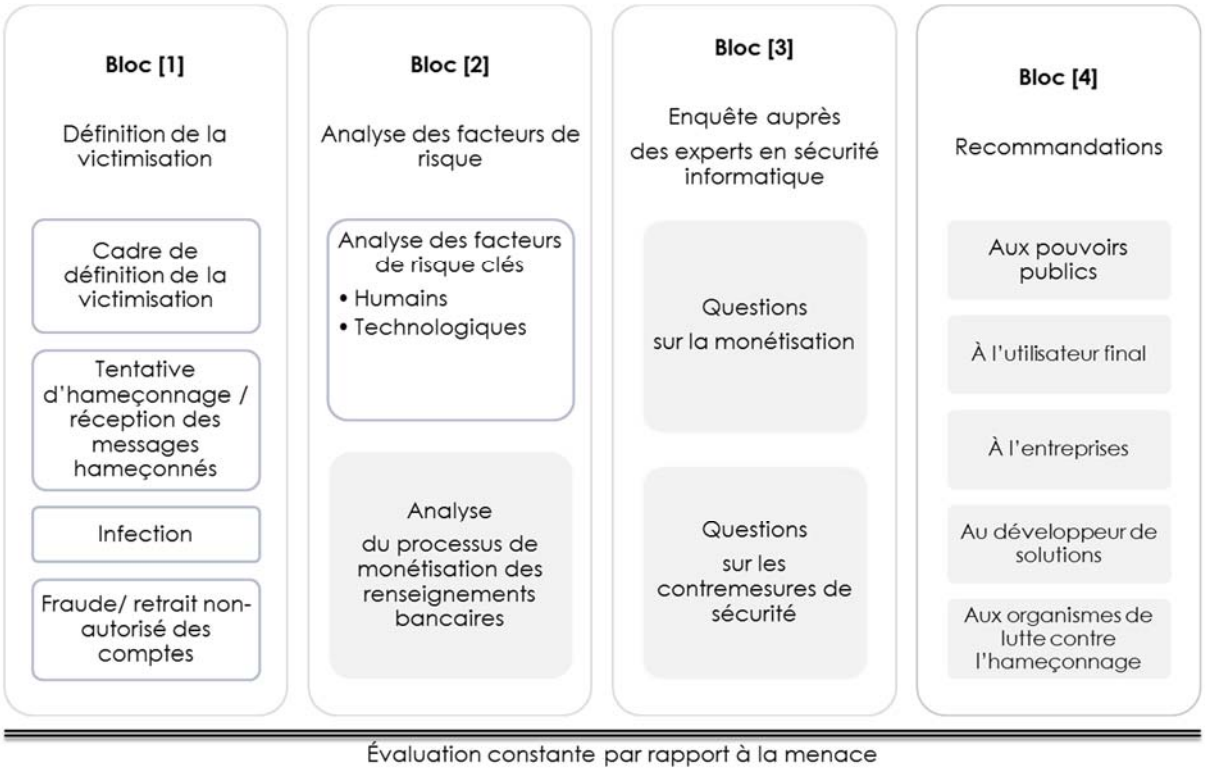


Figure 5.1 : Cadre d'analyse et de réduction de risque d'hameçonnage bancaire proposé

CHAPITRE 6 ANALYSE MICRO-ÉCONOMIQUE DE LA MONÉTISATION DES RENSEIGNEMENTS VOLÉS PAR HAMEÇONNAGE

Ce chapitre présente un modèle micro-économique d'équilibre partiel qui analyse le comportement du fraudeur au cours de l'activité de monétisation des renseignements bancaires sur les cybermarchés clandestins.

Les analyses de la statique comparative montrent que six variables influent sur la monétisation. Il y a le revenu anticipé, l'intensité du niveau de sécurité, la commission versée à la mule, le prix du renseignement, la richesse initiale du fraudeur et la probabilité de se faire arrêter. Parmi ces facteurs, la commission versée à la mule, l'intensité du niveau de sécurité et le prix d'achat du renseignement ont un effet négatif sur les quantités monétisées alors que le revenu anticipé et la probabilité sont deux fonctions croissantes de q.

Notre modèle montre qu'il n'existe pas de combinaisons de valeurs de facteurs exogènes qui assurent un équilibre dans l'activité de monétisation. Cette situation influence les choix des fraudeurs et rend leurs comportements imprévisibles.

Bien que ce modèle soit théorique et que les résultats soient à prendre avec prudence, il révèle à tout le moins, l'importance de la fonction d'utilité du fraudeur dans ce processus de monétisation.

6.1 Introduction

Nous avons défini au chapitre 1, la fraude bancaire comme une chaîne d'activités que l'on peut regrouper en cinq phases : il y a l'envoi du message hameçonné, sa réception, la compromission de la victime, le vol de renseignements et la fraude en tant qu'action de retirer l'argent du compte de sa victime ou d'effectuer des achats avec ses renseignements.

Pour chaque phase, nous avons évalué les facteurs qui contribuent à sa réussite avec pour objectif d'aider à répondre à la préoccupation, très répandue parmi les acteurs qui luttent contre l'hameçonnage bancaire, de savoir si les contremesures mises en œuvre contre ce crime ciblent les

facteurs clés de risque. Pour ce faire, nous avons utilisé des données de l'enquête ESG[57] pour identifier, au chapitre 5, un certain nombre de facteurs pour les quatre premières phases. Restent la phase de fraude et le processus de monétisation y afférent pour laquelle nous ne disposons pas de données factuelles. Nous proposons donc dans ce chapitre, une analyse micro-économique du comportement d'un acteur clé de ce secteur du marché noir des renseignements : le fraudeur.

6.2 Contexte de l'analyse micro-économique

L'examen de la littérature faite au chapitre deux a permis d'identifier entre autres facteurs contributifs au processus de monétisation des renseignements, la richesse initiale du fraudeur, le niveau de sécurité que procurent les contremesures mises en place par les institutions bancaires, les coûts de monétisation, la probabilité de se faire arrêter et les amendes qui en découleraient. Notre objectif étant d'aider à comprendre d'une part, le comportement du fraudeur au moment de monétiser les renseignements volés et, d'autre part, de mieux cerner les interactions entre parties prenantes du processus de monétisation dans un marché noir de renseignements, nous avons choisi d'analyser, à travers un modèle microéconomique, les impacts des variations de chacun de ces facteurs sur le développement de ce marché. Ainsi, les connaissances qui découleront de ces analyses pourront être utilisées pour améliorer l'efficacité des mesures mises en place pour lutter contre la fraude bancaire par hameçonnage.

Les différentes approches économiques d'analyse de la cybercriminalité que nous avons consultées s'appuient sur les travaux de (Becker, 1968; Kopp, 2002; Kshetri, 2006; Herley & Florêncio, 2010). Certains de ces travaux analysent les facteurs économiques des attaques de cybercriminalité, notamment, le comportement et les motivations économiques des attaquants et des défenseurs ainsi que leurs impacts sur l'efficacité des contremesures de façon générale.

Notre modèle se focalise sur une seule facette du marché de la cybercriminalité, celui de la monétisation des renseignements volés par hameçonnage. Il permet de comprendre comment le fraudeur maximise son utilité en présence d'incertitude. Nous y analysons en profondeur le comportement du fraudeur en nous appuyant sur deux éléments fondamentaux : en considérant que le fraudeur, comme tout agent économique ayant des ressources limitées, cherche à maximiser son

[57] Enquête de Statistique Canada

utilité sous deux types de contraintes, l'une budgétaire et l'autre ayant trait aux contremesures de sécurité mises en place par les banques. Ensuite, le modèle prend en compte les préférences du fraudeur. La combinaison des préférences du fraudeur et des contraintes précitées déterminent alors le choix des facteurs à privilégier par le fraudeur afin de maximiser son utilité.

Avant de procéder à la modélisation comme telle, il nous faut dans un premier temps décrire l'approche que nous allons adopter pour étudier le comportement du fraudeur dans ce marché noir.

6.3 Choix de l'approche de modélisation

L'approche de modélisation que nous utilisons pour étudier le comportement du fraudeur s'appuie sur la théorie du choix rationnel qui stipule que l'agent économique cherche le meilleur moyen de maximiser sa satisfaction. Parmi les hypothèses avancées pour défendre cette théorie, il y a celle de Garry Becker (Becker, 1968) à l'effet que «les criminels agissent rationnellement dans les situations où les bénéfices de leurs crimes surpassent la probabilité d'arrestation, de condamnation et de peine de prison ou d'amende». C'est sur cette hypothèse que nous construisons notre modèle.

La première étape de notre modélisation consiste à délimiter le segment du marché que nous voulons étudier, à bien définir les variables qui caractérisent le comportement du fraudeur et celui de la mule, à bien poser le problème de maximisation économique du fraudeur sous deux contraintes : le budget et les contremesures. Puis, à définir la forme fonctionnelle de sa fonction d'utilité. Pour cela, nous avons choisi d'utiliser la fonction d'utilité classique de type CRRA (*Constant Relative Risk Aversion)* pour le cas du fraudeur averse au risque et la fonction d'utilité classique de type CARA (Constant Absolute Risk Aversion) pour le fraudeur qui aime le risque.

La seconde étape est celle de la simulation du modèle mathématique obtenu. Nous utilisons à cet effet le logiciel MathLab pour la statique comparative et le logiciel d'analyse des risques et décision par simulation de Monte Carlo @RISK de Palissade.

Enfin, à la dernière étape, nous interprétons les résultats et nous nous intéressons aux conséquences quant aux contremesures à prendre.

6.4 Secteurs économiques

Le marché souterrain des renseignements représente une économie à deux secteurs : il y a le secteur des renseignements, des produits et services de cybercriminalité et celui du travail au noir.

Le secteur des renseignements et services est constitué, entre autres, de renseignements volés/vendus/achetés et des ressources de «*monétisation*[58]», notamment, les accessoires et machines de clonage. Nous postulons que le fraudeur y achète des renseignements qu'il cherche à convertir « monétiser » en utilisant les services d'une mule. Ces services de mule sont offerts dans un autre secteur du même marché : celui du travail. Le modèle théorique développé dans ce document analyse les comportements des deux agents économiques qui interagissent dans ce second secteur du marché : le fraudeur et la mule[59].

6.5 Fondement microéconomique

Dans le secteur du travail au noir, le fraudeur tire profit uniquement des montants d'argent qR qu'il arrive à soutirer des comptes des victimes, q étant le nombre de renseignements monétisés et R[60] le montant soutiré par renseignement. Il achète Q renseignements[61] au secteur des renseignements du même marché qu'il tente de monétiser. Pour ce faire, le fraudeur a besoin d'une richesse initiale r. Il devra aussi assumer un certain nombre de frais et de dépenses Z(Q) notamment pour payer les services des intermédiaires et/ou pour acquérir des ressources nécessaires à l'activité de monétisation.

De son côté, la mule a un comportement d'offre. Elle offre au fraudeur un niveau d'intensité de l'effort maximal pour monétiser les renseignements pendant une période de temps donnée. En contrepartie, le fraudeur lui verse une commission wR qui dépend positivement de la quantité d'argent R soutiré du compte de la victime, w étant un nombre positif compris entre 0 et 1 (% du revenu payé en commission). Pour simplifier notre modèle, nous supposons qu'on a une mule par renseignement monétisé.

---

[58] On entend par «monétisation», l'ensemble des actions qui concourent à soutirer de l'argent ou à tirer avantage d'un produit/service bancaire en utilisant des renseignements dérobés par hameçonnage auprès des victimes et vendus dans des forums clandestins.

[59] Dans cette thèse, nous considérons la commission versée à la mule comme un coût de monétisation, faisant ainsi abstraction de sa fonction d'utilité.

[60] R est aussi appelé provision ou « balance », c'est le montant que le fraudeur peut retirer du compte de la victime en utilisant les renseignements bancaires. Ce montant est la différence entre la limite maximale autorisée et le solde du compte à un instant bien défini.

[61] Un numéro de carte de crédit, de compte personnel ou de tout autre produit bancaire.

D'autre part, la fraude bancaire étant une activité risquée, la probabilité de se faire arrêter et d'être condamné est p. Lorsqu'on se fait prendre, l'unique pénalité réside dans l'amende S(q). Dans le reste du document, nous utiliserons l'expression *probabilité de se faire arrêter* pour signifier *probabilité de se faire arrêter et d'être condamné*.

Un fraudeur qui veut se faire plus d'argent achète un certain nombre de renseignements Q au marché noir puis tente d'en tirer le maximum de gain possible. Son problème économique de base est donc celui de la maximisation de l'utilité que lui procurent les renseignements qu'il arrive à monétiser sous deux contraintes. La contrainte C_1 que son niveau de profit en l'absence d'amende soit supérieur à zéro et, le cas échéant, la contrainte C_2 que ce niveau de profit soit supérieur au montant de l'amende en cas d'arrestation. Le problème s'écrit formellement comme suit :

$$\begin{cases} \max\limits_{q} E[U] = \max\limits_{q} \left(pU[X] + (1-p)U[Y]\right), \\ C_1: \quad X > 0 \\ C_2: \quad Y > 0 \end{cases} \tag{1}$$

où U est la fonction d'utilité du fraudeur, X est la richesse finale du fraudeur quand il n'est pas pris et Y la richesse finale quand il est découvert[62]. Nous définissons X et Y ci-dessous :

$$X = \underbrace{\mathrm{r}}_{\text{richesse initial}} + \underbrace{\mathrm{Rq}(1-\mathrm{w})(1-\beta)}_{\text{revenus}} - \underbrace{\mathrm{Z(Q)}}_{\text{coûts}} \tag{2a}$$

$$Y = \mathrm{r} + \mathrm{Rq}(1-\mathrm{w})(1-\beta) - \mathrm{Z(Q)} - \underbrace{\mathrm{S(q)}}_{\text{amende}} \tag{2b}$$

Avec Z(Q) qui représente la somme des coûts d'achat des renseignements et des coûts de monétisation. En supposant que ces coûts évoluent de façon linéaire, on peut écrire :

$$\mathrm{Z(Q)} = \mathrm{aQ} + \mathrm{b} \tag{3}$$

où a, représente le prix de chaque unité de renseignement et b le coût d'achat du matériel de clonage par renseignement, le cas échéant.

---

[62] Nous avons supposé que le fraudeur est découvert après avoir soutiré de l'argent du compte. Par conséquent, son revenu est pris en compte dans l'équation de Y.

La réalisation du maximum de profit pour le fraudeur se heurte aussi à une autre contrainte : la contrainte des contremesures de sécurité mises en place par les institutions financières pour réduire les impacts de la monétisation. β, est la variable associée au niveau de sécurité que procure l'ensemble de ces contremesures (0 étant le niveau le plus faible –*aucune contremesure* - et 1 le niveau le plus élevé -*protection maximale*-).

En supposant que l'amende S(q) est une fonction linéaire, qui croit avec le montant total qR dérobé des comptes, on peut écrire S(q)=kRq où k est taux de l'amende et est compris entre 0 et 1.

En remplaçant (3) et S(q) dans (2a) et (2b), on obtient :

$$X = r + R(1-\beta)(1-w)q - aQ - b \quad (4a)$$

$$Y = r + R(1-\beta)(1-w)q - aQ - b - kRq \quad (4b)$$

La détermination du niveau optimal de profit du fraudeur, par maximisation de l'utilité espérée du profit, est obtenue lorsque les conditions suivantes sont satisfaites :

- la dérivée première de l'utilité espérée doit être nulle, $E[U'] = \frac{\partial E[U]}{\partial q} = 0$ et,
- on doit aussi vérifier que la dérivée seconde est négative, soit $E[U''] = \frac{\partial^2 E[U]}{\partial q^2} < 0$

D'une part, $si\ q^*$ est le nombre de renseignements fraudés à l'optimum, on le trouve en prenant la condition de premier ordre :

$$\frac{\partial E[U]}{\partial q} = pU'[X]\frac{\partial X}{\partial q} + (1-p)U'[Y]\frac{\partial Y}{\partial q}) = 0 \quad \Leftrightarrow$$

$$pU'[X][R(1-\beta)(1-w)] + (1-p)U'[Y][R(1-\beta)(1-w) - kR] = 0 \quad (5)$$

D'autre part, pour vérifier que la dérivée seconde est négative à l'équilibre, on pose :

$$\frac{\partial^2 E[U]}{\partial q^2} = D_q \text{ où } D_q\ est \text{ négatif.} \quad (6)$$

En remplaçant (5) dans (6), on obtient la forme générale suivante :

$$\frac{\partial}{\partial q}\left(\frac{\partial E[U]}{\partial q}\right) = \frac{\partial}{\partial q}(pU'[X][R(1-\beta)(1-w)] + (1-p)U'[Y][R(1-\beta)(1-w) - kR]) = D_q \quad (7)$$

Rappelons que notre objectif est de capter l'effet de changement de la solution q lorsqu'un des paramètres exogènes varie. En d'autres termes, nous voulons analyser le comportement du fraudeur en étudiant l'effet des variations de chaque paramètre exogène sur la seule variable que le fraudeur contrôle, q. Toutefois, en observant bien la forme générale obtenue en (7), on s'aperçoit que nous ne connaissons pas la forme de U. Nous postulons que cette fonction, encore appelée fonction d'utilité, doit être conforme au comportement du fraudeur et refléter son attitude vis-à-vis du risque.

6.6 Attitude du fraudeur vis-à-vis du risque

Nous supposons que le fraudeur, comme toute personne rationnelle, n'investit son temps et son argent que s'il espère faire un profit. Nous supposons en outre que le fraudeur est soit adverse au risque «risquophobe», soit neutre ou alors il aime le risque «risquophile». U peut donc prendre trois formes.

Nous postulons qu'on peut trouver une solution à l'équation (7) en imposant des formes fonctionnelles. Pour cela, on a besoin d'émettre des hypothèses sur l'attitude du fraudeur face au risque.

6.6.1 Le fraudeur est averse au risque

Pour analyser son comportement vis-à-vis du risque, nous avons choisi d'utiliser la fonction d'utilité classique CRRA (*Constant Relative Risk Aversion*) définie comme suit :

$$\mathrm{U(X)} = \begin{cases} \frac{\mathrm{X}^{(1-\mathrm{e})}}{(1-\mathrm{e})} & \text{si } \mathrm{X} > 0, \mathrm{e} \neq 1 \\ \ln \mathrm{X} & \text{si } \mathrm{e} = 1 \end{cases} \tag{8}$$

où $e \in [0,1]$, représente l'indice relatif d'aversion au risque (IRAR)

En remplaçant (8) dans (5), et par manipulation, la condition de premier ordre prend la forme générale suivante pour un fraudeur averse au risque :

$$\frac{\partial \mathrm{E}}{\partial \mathrm{q}} = -\frac{(\mathrm{R}*\mathrm{k} - \mathrm{R}*(\beta-1)*(\mathrm{w}-1))*(\mathrm{p}-1)}{\mathrm{b}-\mathrm{r}+\mathrm{Q}*\mathrm{a}+\mathrm{R}*\mathrm{k}*\mathrm{q}-\mathrm{R}*\mathrm{q}*(\beta-1)*(\mathrm{w}-1)} - \frac{\mathrm{R}*\mathrm{p}*(\beta-1)*(\mathrm{w}-1)}{\mathrm{b}-\mathrm{r}+\mathrm{Q}*\mathrm{a}-\mathrm{R}*\mathrm{q}*(\beta-1)*(\mathrm{w}-1)} \tag{9}$$

En procédant de même pour les équations (8) et (7), la condition de second ordre donne la forme suivante :

$$\frac{\partial^2 E}{\partial q^2} = \frac{\left(R*k - R*(\beta-1)*(w-1)\right)^2*(p-1)}{\left(b - r + Q*a + R*k*q - R*q*(\beta-1)*(w-1)\right)^2} - \frac{R^2*p*(\beta-1)^2*(w-1)^2}{\left(b - r + Q*a - R*q*(\beta-1)*(w-1)\right)^2} - D_q = 0 \qquad (10)$$

La solution qui vérifie l'équation (9) est q*(a, b, Q, *p*, R, β, w, r). Or, Q et b sont constants du fait qu'ils représentent respectivement la quantité de renseignements achetés au marché noir et le coût d'achat du matériel de clonage. Reste alors 6 paramètres exogènes dont dépend cette solution, notamment, la probabilité de se faire prendre *p*, le montant d'argent en jeux R (revenu anticipé par renseignement), le niveau de sécurité que procurent les contremesures β, la commission versée à la mule w, le prix de chaque unité de renseignement a et k, le taux de l'amende . Or, k et w sont des ratios (%) de R, donc ce sont des variables dépendantes.

6.6.2 Le fraudeur est neutre vis-à-vis du risque

Pour analyser le comportement du fraudeur qui est neutre vis-à-vis du risque, nous avons choisi d'utiliser la fonction d'utilité U(X) tel que $U(X) = X \quad et\ U'(X) = 1$

Pour un fraudeur neutre vis-à-vis du risque, la condition de premier ordre prend la forme générale suivante :

$$\frac{\partial E}{\partial q} = \left(R * k - R * (\beta - 1) * (w - 1)\right) * (p - 1) + R * p * (\beta - 1) * (w - 1) \qquad (11)$$

Comme la condition de premier ordre ne dépend pas de q, il n'est donc pas possible, dans ces conditions, d'étudier le comportement d'un fraudeur neutre vis-à-vis du risque.

6.6.3 Le fraudeur aime le risque

Pour analyser le comportement d'un fraudeur qui aime le risque, nous avons choisi d'utiliser une fonction d'utilité usuelle de type CARA (*Constant Absolute Risk Aversion*) et dont la forme générale s'écrit :

$U(X) = \exp(-iX) \quad \text{avec } i = -1,$

où i représente l'indice absolu d'aversion au risque (IAAR).

En supposant que la dérivée de son utilité U est continue et strictement positive, on peut écrire:

$$U'(X) = \exp(X) > 0$$

La condition de premier ordre prend la forme générale suivante pour un fraudeur qui aime le risque :

$$\frac{\partial E}{\partial q} = \exp\big(r - b - Q * a - R * k * q + R * q * (\beta - 1) * (w - 1)\big) * \big(R * k - R * (\beta - 1) * (w - 1) * (p - 1)\big) + R * p * \exp(r - b - Q * a + R * q * (\beta - 1) * (w - 1)) * (\beta - 1) * (w - 1) = 0 \quad (12)$$

Quant à celle de second ordre, elle prend la forme suivante :

$$\frac{\partial^2 E}{\partial q^2} = R^2 * p * \exp\big(r - b - Q * a + R * q * (\beta - 1) * (w - 1)\big) * (\beta - 1)^2 * (w - 1)^2 - \exp\big(r - b - Q * a - R * k * q + R * q * (\beta - 1) * (w - 1)\big) * \big(R * k - R * (\beta - 1) * (w - 1)\big)^2 * (p - 1) - Dq = 0 \quad (13)$$

On applique le même raisonnement exposé au paragraphe sur le fraudeur averse au risque et on en tire des conclusions analogues par rapport à la solution q* qui vérifie cette équation, c'est-à-dire qu'elle dépend de six paramètres exogènes qui sont a, *p*, R, β, w et r.

À ce stade de notre démarche, on a besoin de comparer les différents états d'équilibre, avant et après changement de chacun des paramètres ci-dessus afin de comprendre les interactions entre le fraudeur et ce marché. Pour y arriver, nous émettons ci-dessous un certain nombre d'hypothèses de simulation.

6.7 Hypothèses de simulation

6.7.1 Probabilité de se faire arrêter et d'être condamné «p»

Les études consultées nous apprennent que les taux d'arrestation et de condamnation pour cyber-fraude bancaire sont très faibles. L'arrestation des suspects étant d'autant plus difficile que les cybercriminels fonctionnent tous sous anonymat quand ils ne se trouvent pas à l'autre bout du

monde. Par exemple, N. Kshetri estime la proportion de vols d'identité par Internet à moins de 1 sur 700 (Kshetri, 2006). À défaut d'autres chiffres, nous nous sommes basés sur cette estimation de (Kshetri, 2006) pour établir notre intervalle de valeurs de simulation de p entre 1/1000 et 1/100.

Nous postulons donc que :

- le fraudeur et la mule se font confiance, ce qui veut dire que la probabilité que la mule fraude le fraudeur est presque nulle;
- les tentatives de fraude sont des évènements indépendants;
- plus le nombre de renseignements q augmente, plus le risque de se faire attraper et condamner est élevé.

H6.1 : la quantité monétisée q est une fonction croissante de la probabilité de se faire arrêter.

6.7.2 Niveau de sécurité β

Les institutions émettrices des cartes bancaires prennent des mesures conformes aux normes de l'industrie bancaire pour lutter contre la fraude en ligne. Ces mesures sont appliquées de la même façon pour tous les comptes clients, garantissant ainsi le même niveau de sécurité pour tous. Toutefois, certaines méthodes d'authentification semblent plus perfectionnées que d'autres. Par exemple, Murdoch et al. préconisent d'ajouter au système 3D[63] Sécure très utilisé par les banques en ce moment, une étape supplémentaire d'authentification de la transaction et/ou la signature électronique (Murdoch & Anderson, 2010).

Nous utilisons notre modèle pour tenter d'étudier l'effet de la variation du niveau de sécurité, β, que procurent ces méthodes mises en place par certaines institutions financières pour protéger les renseignements personnels. Nous supposons intuitivement (en l'absence de données réelles) :

- qu'il y a deux niveaux de sécurité, un niveau de base sans authentification des transactions et un niveau avec authentification des transactions (cf. Tableau 6.1);
- que plus le niveau de sécurité augmente, moins élevées sont les quantités monétisées q.

[63] C'est un programme connu pour les cartes Visa sous le nom "Verified by Visa" et, pour les cartes Mastercard, sous le nom "Mastercard Secure Code". Il ajoute une étape de plus au processus de paiement en ligne, étape qui consiste à exiger qu'un code d'authentification à usage unique soit renvoyé (via sms par exemple) pour finaliser la transaction.

Ce postulat s'appuie sur les informations colligées sur les sites web des institutions émettrices de cartes de crédit et s'inspire des conclusions de l'article de Murdoch et Anderson (Murdoch & Anderson, 2010) qui recommande d'ajouter, au système 3DS, une étape d'authentification de la transaction qui demanderait par exemple au client: "*Vous êtes sur le point de payer X $ pour le marchand Y. Si cela est correct, entrez le code d'authentification*"(Murdoch & Anderson, 2010).

Tableau 6.1 : Niveaux de sécurité opérationnelles mise en place par les banques

Béta (β) Niveau de sécurité	**Explication**
Niveau de base (sans authentification)	Coupe-feu, chiffrement, témoins[64], mot de passe, NIP, questions de sécurité, les codes d'accès, surveillance proactive, carte à puce, etc.
Niveau avec authentification	Authentification de transaction en ligne par des protocoles comme 3D-Secure ou Verified By Visa et MasterCard SecureCode, authentification biométrique, etc.) ou signature électronique, etc.

Nous pouvons donc formuler notre troisième hypothèse comme suit :

H6.3 : plus le niveau de sécurité augmente, moins élevées sont les quantités monétisées q.

Nous y reviendrons au paragraphe consacré à la statique comparative.

6.7.3 Commission versée à la mule «w»

Le choix d'étudier ce facteur est conforté par la place qu'occupe la mule dans le «*pipeline*» de la fraude : sans elle, les renseignements volés n'ont que peu de valeurs (Florêncio & Herley, 2010). Nous pensons donc que la commission versée à la mule devrait refléter cette importance. Notre intuition est à l'effet que plus la commission versée à la mule est attrayante, plus la mule est prête à prendre davantage de risques et plus ses efforts sont récompensés, toutes choses égales par ailleurs. Notre hypothèse est que :

[64] C'est un fichier contenant des éléments d'information que le site Web de la banque crée automatiquement lorsqu'un client le visite. Par exemple, lorsqu'un client se connecte à «service Net» d'une banque, le serveur du «service Net» capture ces informations et pendant toute la durée de la session d'utilisation, il fait les vérifications nécessaires pour s'assurer que la banque fait affaire avec le bon client.

H6.4 : la quantité monétisée q est une fonction croissante de la commission versée à la mule.

6.7.4 Prix du renseignement «a»

Enfin, il y a l'effet de variabilité du prix du renseignement sur la quantité q que nous devons étudier. Pour ce faire, nous postulons que :

- les effets de distorsions des prix entre forums « market distortions » et de distorsions des recettes entre un fraudeur expérimenté et un fraudeur novice «Spence distortion» sont négligeables;
- le prix du renseignement prend la forme d'un continuum de prix influencés par un certain nombre de caractéristiques, notamment : la durée entre la brèche de sécurité et la mise en marché de ces informations, le détail des renseignements personnels sur le détenteur de la carte, la réputation du vendeur, etc.;
- plus le prix du renseignement est élevé, meilleure est la qualité du renseignement et plus élevées sont les chances de le monétiser et plus q augmente.

H6.5 : plus le prix du renseignement est élevé et plus élevées sont les chances de le monétiser.

6.7.5 Richesse initiale «r»

La richesse initiale du fraudeur nous renvoie à la notion de «capacité[65]» qui, combinée avec la motivation et l'opportunité, contribuent à l'occurrence d'une fraude (Cressey, 1986). On entend ici par capacité, la connaissance, les outils et les ressources humaines et monétaires nécessaires à la réalisation d'une fraude. Pour étudier l'effet de la variabilité de la richesse initiale du fraudeur sur la quantité q que le fraudeur peut monétiser, nous nous sommes inspirés de ce qui se fait dans le milieu de la criminalité traditionnelle où la hausse marquée de la richesse personnelle contribue à créer de plus en plus d'opportunités pour l'acte criminel (Kitchen, 2006). Nous supposons donc que le fraudeur qui a une richesse initiale plus importante est plus à même d'acheter les

[65] Fait référence à l'un des trois éléments du triangle de la fraude tels qu'identifiés par Donald Cressey comme étant précurseurs d'activités frauduleuses. Il s'agit de la motivation, de la capacité et de l'opportunité.

renseignements de qualité et donc d'augmenter sa capacité d'attaque. Notre hypothèse se formule donc comme suit :

H6.6 : plus la richesse initiale du fraudeur est élevée, plus grandes sont ses chances de monétiser les renseignements.

6.8 Données de simulation

D_Q : Cette variable est utilisée à des fins de manipulation mathématique dans la résolution de la condition de second ordre à l'équilibre (cf. équation (6)). Elle prend la valeur -1.

p : C'est la probabilité de se faire prendre et d'être condamné. À défaut de disposer des chiffres plus récents, nous nous inspirons des données sur la probabilité issues du livre de N. Kshetri (Kshetri, 2010). On peut y lire que la proportion de vols d'identité est estimée à moins de 1 sur 700 tandis que le FBI estime la probabilité d'être condamné à 1 contre 22,000. Nous postulons que cette variable suit une loi triangulaire avec 1/700 comme valeur probable.

T [1/1000, 1/700, 1/100]

β : Niveau de sécurité. Bien qu'il n'existe pas de niveau nul ou de niveau maximal en sécurité (risque nul n'existe pas), nous avons choisi, pour des fins de simulation une loi triangulaire et un intervalle de valeurs théoriques pour le niveau de sécurité compris entre 0.1 et 0.99 avec comme valeur probable 90%. Cette valeur correspond à la proportion de détection de la fraude bancaire réalisée par les contremesures d'arrière-plan (back-end) (Florêncio & Herley, 2010).

T [0.1, 0.9, 0.99]

R : C'est le montant d'argent qu'un fraudeur peut soutirer du compte de la victime. Nous nous sommes inspirés des données sur les limites de cartes de crédit de Visa pour définir notre intervalle de valeurs de simulation compris entre 500 $ et 10 000 $, 500 $ étant la limite de crédit minimale que les banques autorisent, 1500 $ la limite de retrait par jour (valeur probable) et 10 000 $ la limite maximale dans notre cas de figure.

T [500 $, 1500 $, 10000 $]

a : C'est le prix d'achat de chaque renseignement. Il varie entre 0.40 $ et 100 $ (Wueest, 2015). 0.40 $ correspond à un renseignement de moins bonne qualité alors qu'avec 100 $ on peut se procurer un renseignement d'excellente qualité. Rappelons que la qualité ici fait référence à l'effet combiné de l'origine et du type du renseignement, des options qu'il offre (platine, or, etc.), de sa durée sur le marché, du solde disponible, du code de sécurité et des informations personnelles du détenteur. Plus un renseignement a tous ces éléments, meilleure est sa qualité.

T : [0.40 $, 0.50 $, 100 $]

r : C'est la richesse initiale du fraudeur. Nous avons intuitivement choisi l'intervalle de valeurs entre 40 $ et 400 $, en se basant sur le prix du renseignement et du nombre de renseignements que nous utilisons pour fin de simulation.

T : [40 $, 50 $, 400 $]

b : Coût d'achat du matériel de clonage. Nous avons choisi une valeur constante arbitraire de 50c par renseignement pour des fins de cette simulation.

Q : Quantité de renseignements achetés au marché noir. Nous supposons que le fraudeur a acheté 100 numéros d'un coup.

w : C'est un pourcentage (%) du montant R que le fraudeur verse en commission à la mule. Il est compris entre 0.07 et 0.4 fois le revenu anticipé (R). Ces chiffres nous proviennent de l'article de C. Wueest (Wueest, 2015). Dans cet intervalle, la valeur probable, celle qui revient fréquemment dans les articles lus est de 10%.

T : [0.07, 0.1, 0.4]

Tableau 6.2 : Niveaux de commission versée à la mule

Moyenne commission (w)	Catégorie	Explications
7% - 10%	Basse	% versé à une mule pour monétiser un renseignement provenant d'un autre continent (ex. mule Russe pour une carte nord-américaine) – *monétisation transcontinentale* -
20%	Moyenne	% versé à une mule pour monétiser un renseignement provenant d'un autre pays (ex. carte Canadienne et mule américaine ou carte française et mule Russe) – *monétisation transfrontalière*-
40%	Élevée	% versé à une mule pour monétiser un renseignement provenant du même pays (ex. mule et carte du même pays) - *monétisation nationale*-

6.9 Analyse de statique comparative

L'objet de cette analyse est d'étudier les effets de la variation de la «variable-effet» q*(a, p, R, β, w, r) à l'optimum lorsqu'on agit sur les «variables-causes», ici les paramètres exogènes. Par exemple, on peut se demander quelle va être l'incidence sur les chances de monétiser si l'on ajoute au protocole «*Verified By Visa*» une étape supplémentaire d'authentification de la transaction par signature électronique. Pour tenter de répondre à cette question, nous avons besoin de comparer les différents états d'équilibre, avant et après ajout de cette option de sécurité.

d) Effet de la variation de la probabilité (p)

À titre de rappel, notre hypothèse H6.1 est à l'effet que la quantité monétisée q est une fonction croissante de la probabilité de se faire arrêter. La solution qui vérifie, à l'optimalité, chacune des équations (9) et (12), selon que l'on soit risquophobe q^*_{av} ou risquophile q^*_{rl}, s'écrit :

$$q^*_{av} = -\left(\frac{49}{144} - \frac{1225*p}{2304}\right) \qquad q^*_{rl} = -\frac{\log\left(-\frac{(16*(p-1))}{9*p}\right)}{4000}$$

En comparant deux états d'équilibre, p=0.001 et p =0.01, on s'aperçoit qu'il y a une sensibilité dans la variation de la probabilité de se faire prendre lorsque les quantités à monétiser augmentent. Cette sensibilité est positive et faible comme on peut l'observer sur les deux courbes de la figure 6.1 ci-

dessous. On y voit une pente positive infiniment petite. Notre hypothèse à l'effet que « *la probabilité de se faire arrêter est une fonction croissante de q* » est donc confirmée. Toutefois, la faible croissance indique que son effet n'est pas des plus déterminants dans la décision. Ainsi, la probabilité de se faire prendre affecte légèrement la monétisation, toutes choses étant par ailleurs égales.

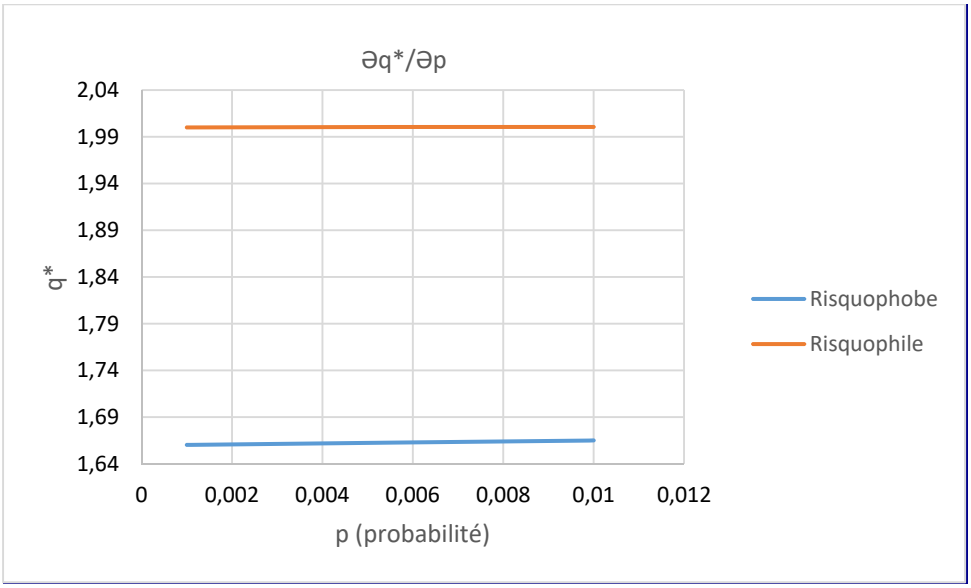


Figure 6.1 : q* est peu sensible à la variation de la probabilité

De plus, cette figure révèle un écart d'amplitude entre les résultats du fraudeur qui aime le risque et ceux de celui qui est averse au risque. Cet écart peut s'expliquer par le fait que le fraudeur qui est averse au risque est « *moins tenté de commettre des crimes que les autres* » (Kopp, 2002).

e) Effet des revenus anticipés (R)

Dans notre hypothèse H6.2, nous postulons que «l'augmentation du revenu anticipé R a un impact positif sur la quantité q de renseignements monétisés». En suivant la même démarche de dérivation qu'en a), on arrive aux expressions de $q^*_{av,}$ q^*_{rl} suivantes :

$$q^*_{av} = -\frac{86975}{64*R^2} \qquad q^*_{rl} = \left(-\frac{\log(1776)}{R}\right)$$

Les résultats de simulation (figure 6.2) révèlent qu'il y a un accroissement significatif des quantités monétisées entre 500 $ et 2000 $, puis, après 2000 $, cet accroissement ralentit progressivement avant de se stabiliser. Ce comportement nous renvoie à la notion de revenu marginal, c'est-à-dire le revenu supplémentaire que génère toute tentative de monétisation d'un renseignement additionnel. L'interprétation que nous en faisons est qu'il est plus aisé pour le fraudeur de soutirer de petites sommes d'argent (soit pour des achats en ligne ou par retrait mais en autant que le montant soit en deçà de la limite quotidienne). Et, lorsque ce plafond est atteint, il devient plus difficile de monétiser davantage. Un résultat qui ne surprend pas car il reflète l'usage quotidien des cartes de crédit sous contrainte des contremesures opérationnelles de sécurité qui plafonnent les achats et limitent les retraits d'argent.

L'autre résultat attendu et qui s'observe dans cette figure est l'écart d'amplitude considérable entre les quantités que peuvent monétiser les fraudeurs risquophile et risquophobe. Ce résultat, tout comme le précédent, était plutôt prévisible car l'appétit pour le gain est plus élevé chez le fraudeur risquophile que chez celui qui est risquophobe.

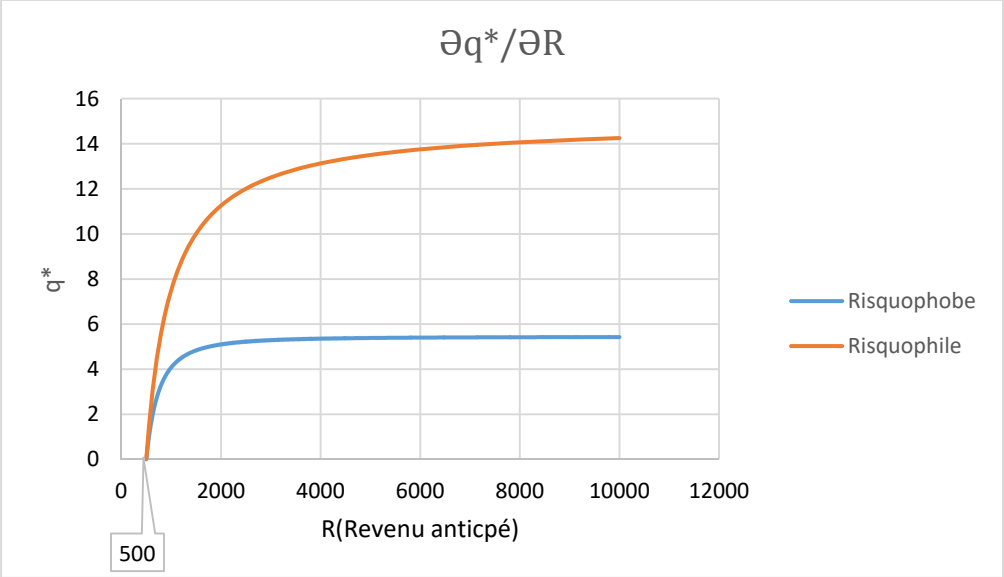


Figure 6.2 : q* croit en fonction du revenu anticipé

Dans l'ensemble, nos résultats de simulation sont en phase avec notre intuition de départ à l'effet que, comme tout agent économique, le fraudeur cherche constamment à maximiser son profit et

l'espérance de faire plus d'argent a un impact positif sur la détermination qu'il a de monétiser davantage de renseignements (q est alors une fonction positive de R).

Cela s'explique en partie par le fait qu'il est plus facile de monétiser de petits montants d'argent qui, plus souvent qu'autrement, passent plus inaperçus chez les victimes et auprès des banques que de gros montants, ces derniers étant surveillés de près par les contremesures opérationnelles mises en place par les banques.

f) Effet de la variation du niveau de sécurité β sur la quantité q

Nous avons postulé dans notre troisième hypothèse H6.3 que «plus le niveau de sécurité augmente, moins élevées sont les quantités monétisées q». En suivant la même démarche de dérivation qu'en a) et en b), on arrive aux expressions de $q^*_{av,}$ q^*_{rl} suivantes :

$$q^*_{av} = \frac{441*\beta + \frac{4851}{100}}{4000*\left(\beta - \frac{81*\beta^2}{100} + \frac{9}{100}\right)} \qquad q^*_{rl} = -\left(\frac{\log\left(-\frac{(111*(3600*\beta+400))}{400*(\beta-1)}\right)}{4000}\right)$$

Les résultats de simulation montrent (cf. Figure 6.3) une décroissance lente de la quantité monétisée lorsque le niveau de sécurité est de bas, avec une pente plus abrupte lorsque le niveau de sécurité avoisine 90%. C'est dire qu'avec des mesures opérationnelles accrues, il est possible de réduire au strict minimum la possibilité de monétiser un renseignement.

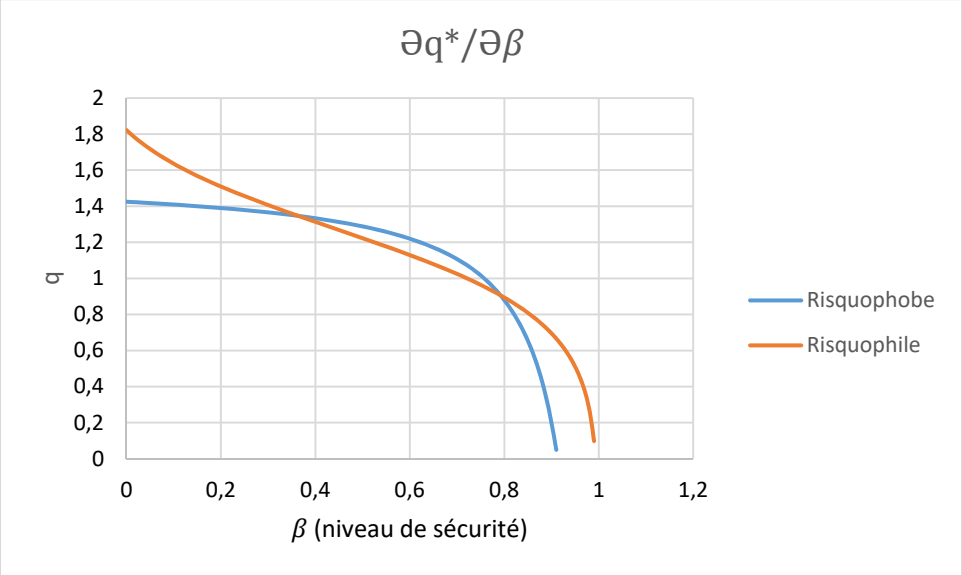


Figure 6.3 : Effets des contremesures de sécurité sur les quantités q*

La différence entre risquophobe et risquophile dans ce cas est peu significative comme on peut le remarquer sur la Figure 6.3.

Les résultats de notre simulation confirment notre hypothèse H6.3 à l'effet que plus le niveau de sécurité augmente, moins élevées sont les quantités monétisées q. L'exemple qui illustre cette hypothèse est l'adoption de la technologie 3D Secure par Visa, MasterCard et les marchands. Avec l'authentification améliorée des transactions que permet ce protocole, la fraude par cartes et les pertes de paiements ont été réduites significativement (GC, 2013). Le corollaire de cette diminution de quantité « *monétisable* » est que les fraudeurs se retrouvent avec des stocks de renseignements et que les prix des renseignements dans les forums clandestins soient bas (Wueest, 2015). Nous y reviendrons dans l'analyse de l'effet de variation des prix des renseignements.

g) Effet de la commission de la mule (w)

Relativement à la commission versée à la mule, nous avons postulé en H6.4 qu'elle était une fonction croissante de la quantité monétisée. C'est-à-dire que plus le montant versé en commission est attrayant, plus la mule prend des risques et plus ses efforts sont récompensés. Pour étudier ce lien potentiel, nous avons résolu par dérivation des équations (9) et (12). On obtient les expressions de $q^*_{av,}\ q^*_{rl}$ suivantes :

$$q^*_{av} = -\left(-\frac{196*w+\frac{29351}{100}}{4000*\left(\frac{(4*w^2)}{25}+\frac{2*w}{25}-\frac{6}{25}\right)}\right) \qquad q^*_{rl} = -\left(-\frac{\log\left(-\frac{(999*(1600*w+2400))}{1600*(w-1)}\right)}{4000}\right)$$

Les courbes de la Figure 6.4 montrent deux tendances : un q* très légèrement en hausse pour le fraudeur risquophile et une courbe décroissante pour le fraudeur risquophobe. Pour le risquophile, notre hypothèse semble vérifiée. En revanche, pour le fraudeur averse au risque c'est l'inverse qui se produit. Un effet négatif de la variation de la commission sur les quantités monétisées invalide notre hypothèse. Ce qui veut dire que plus les commissions des mules sont attrayantes et moins les fraudeurs risquophobes monétisent de renseignements.

Ce résultat semble paradoxal au premier abord, mais il n'en est pas moins vrai que lorsque la commission à verser à une mule est attrayante, c'est généralement parce que le risque de se faire

prendre est tout aussi élevé. En effet, selon (Aston et al., 2009), dans ce secteur du marché noir, certaines mules commettent sciemment leur crime alors que pour d'autres, et c'est dans la plupart des cas, les mules sont des dupes, des agents innocents qui sont exploités par des fraudeurs ou des entreprises criminelles. Dans ce second cas de figure, une commission élevée attise les soupçons de la mule inconsciente et provoque chez cette dernière une attitude de prudence qui peut se traduire par cet effet négatif. Pour les mules qui participent sciemment à la fraude, cet effet peut s'expliquer par le fait qu'une commission élevée est offerte souvent pour des renseignements difficiles à monétiser. Par exemple, un fraudeur aura tendance à offrir une commission élevée lorsque le renseignement qu'il veut monétiser est de moindre qualité ou à haut risque. L'effet négatif sur la quantité que le fraudeur peut monétiser viendrait donc du niveau de difficulté croissant à mesure que la qualité diminue. Nous revenons au paragraphe intitulé discussion sur cette notion de qualité du renseignement.

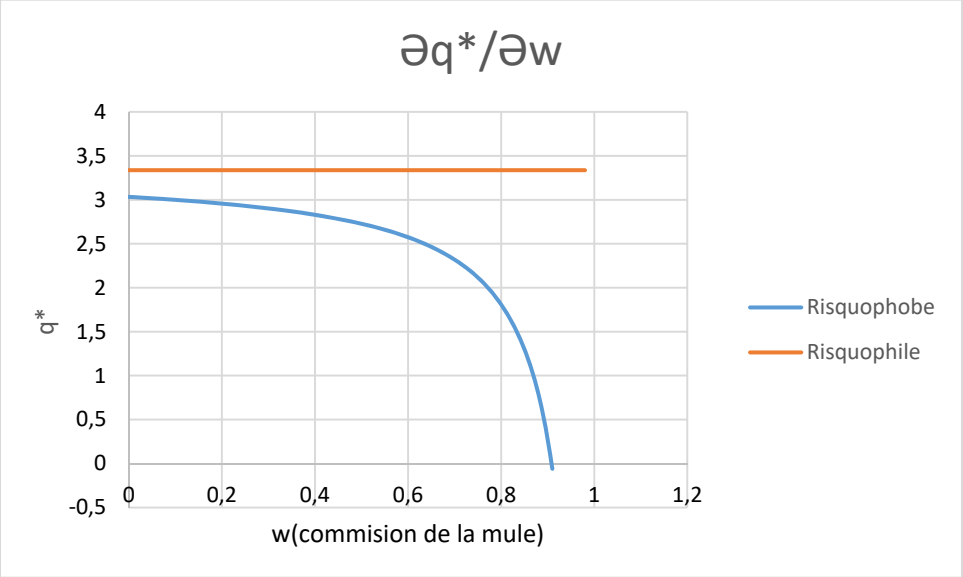


Figure 6.4 : Effet de la variation de la commission versée à la mule sur q*

h) Effet de la variation du prix (a)

Rappelons que notre hypothèse H6.5 est à l'effet que «plus le prix du renseignement est élevé, plus grandes sont les chances de le monétiser et plus q augmente». En suivant la même démarche de dérivation qu'en a), b), c) et d), on arrive aux expressions de $q^*_{av,}$ q^*_{rl} suivantes :

$$q^*_{av} = -\left(\frac{71*a}{1024} + \frac{639}{2048}\right) \qquad q^*_{rl} = -\frac{\log(1776)}{4000}$$

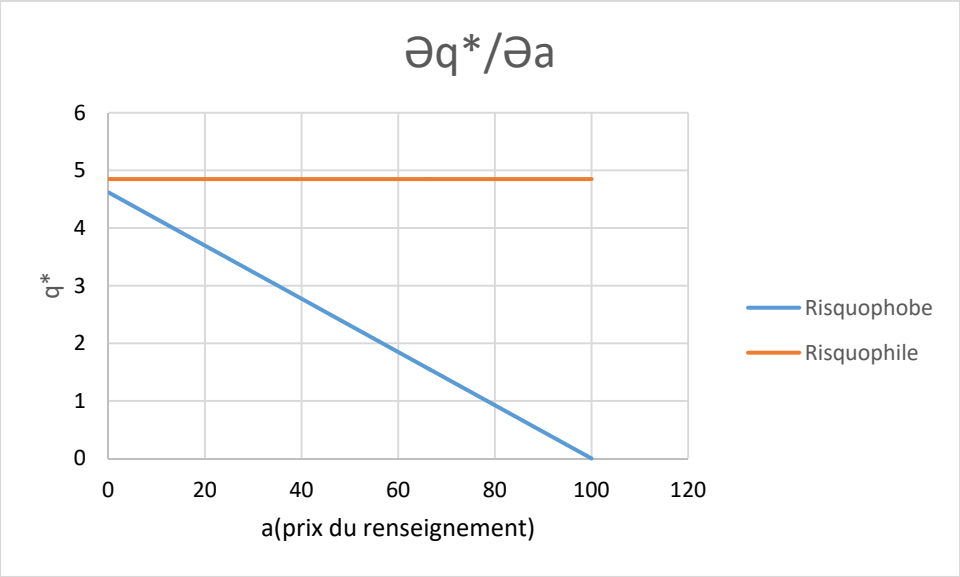


Figure 6.5 : Effet de la variation du prix du renseignement sur q*

Les résultats de simulation montrent deux courbes complètement différentes selon qu'on soit risquopobe ou risquophile. Le fraudeur qui est averse au risque a tendance à monétiser moins lorsque le prix du renseignement est élevé alors que celui qui aime le risque a une attitude plutôt indifférente face au prix d'achat du renseignement (cf. figure 6.5). L'explication que nous pouvons donner est la suivante : comme tout agent économique rationnel, le fraudeur qui a de l'aversion pour le risque préférera un «gain espéré certain» à une situation plus risquée. Ce qui veut dire qu'il aura tendance à monétiser le renseignement qui ne lui coute pas très cher à l'achat afin d'éviter des pertes significatives. C'est un comportement de prudence qui caractérise bien l'individu risquophobe. En revanche, le fraudeur qui aime le risque n'observe pas la même prudence, il cherche à maximiser ses revenus sans égard au prix du renseignement.

Ces résultats invalident donc notre hypothèse H6.5 mais souligne, du même souffle, l'effet de la fonction d'utilité du fraudeur sur les quantités qu'il peut monétiser. Nous y reviendrons plus loin pour tenter de voir s'il y aurait un lien avec la richesse initiale du fraudeur.

i) Effet de la variation de la richesse initiale (r)

Enfin, rappelons que notre hypothèse H6.6 est à l'effet que «plus la richesse initiale du fraudeur est élevée plus grandes sont ses chances de monétiser les renseignements». En suivant la même démarche de dérivation qu'en a), b), c), d) et e), on arrive aux expressions de $q^*_{av,}$ q^*_{rl} suivantes :

$$q^*_{av} = -\left(\frac{1917}{5120} - \frac{(71*r)}{102400}\right) \qquad q^*_{rl} = -\frac{\log(1776)}{4000}$$

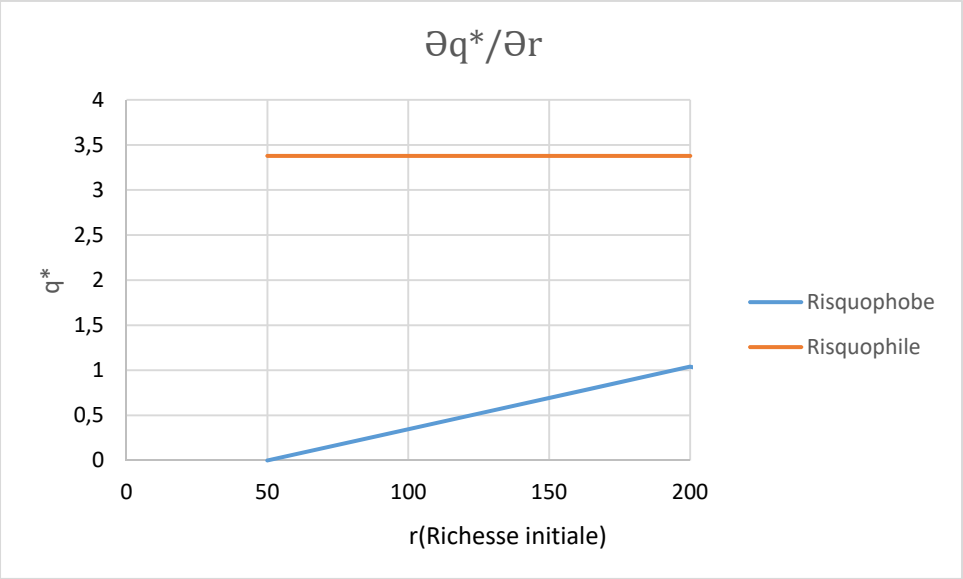


Figure 6.6 : Effet de la richesse initiale du fraudeur sur q*

Les résultats de simulation montrent deux cas de figure distincts : d'un côté, on observe que la hausse de la richesse initiale du fraudeur risquophile n'a pas d'effet sur la quantité qu'il peut monétiser et, de l'autre, on voit que le comportement du risquophobe confirme notre hypothèse H6.6, toutes choses étant égales par ailleurs (cf. figure 6.6). La quantité qu'il peut monétiser croit légèrement à mesure que sa richesse initiale augmente. À l'instar du prix du renseignement, la richesse initiale semble affecter le même facteur d'occurrence de la fraude : la capacité. Le prix du renseignement étant un coût, son augmentation réduit la capacité du fraudeur alors que la hausse de la richesse initiale accroit cette même capacité puisqu'il constitue en soi un investissement.

Pour compléter cette analyse de la statique comparative, nous avons résumé dans le tableau 6.3 ci-dessous les effets de variation de tous les différents facteurs exogènes de notre modèle sur les quantités monétisées q.

Tableau 6.3 : Récapitulatif des résultats de statique comparative

		Probabilité de se faire arrêter (p)	Revenus anticipés (R)	Niveau de sécurité (β)	Commission mule (w)	Prix (a)	Richesse (r)
q*	Risquophobe	+	+	-	-	-	+
	Neutre vis-à-vis	N/A					
	Risquophile	+	+	-	-	0	0

Les signes utilisés dans ce tableau donnent le sens de l'effet de la variation des paramètres exogènes sur les quantités monétisées (q*).
(+) indique un effet positif de la variation du paramètre exogène sur q^*
(-) indique un effet négatif de la variation du paramètre exogène sur q^*
(0) indique que la variation du paramètre exogène n'a aucun effet sur q^*
N/A veut dire qu'il n'a pas été possible d'étudier le comportement d'un fraudeur neutre vis-à-vis du risque.

La lecture de ce tableau révèle que la probabilité de se faire arrêter, les revenus anticipés par le fraudeur ou sa richesse initiale ont chacun un effet positif sur les quantités monétisées q lorsque le fraudeur est risquophobe. En revanche, lorsqu'il est risquophile, seuls les deux premiers facteurs ont chacun un effet positif, le troisième facteur, c'est-à-dire la richesse initiale, n'ayant pas d'effet sur la quantité monétisée. Aussi, nous observons que le renforcement du niveau de sécurité par les banques et l'augmentation de la commission versée aux mules semblent plutôt avoir des effets négatifs sur la monétisation, toutes choses égales par ailleurs.

Au vu de ces résultats, nous sommes en mesure de dire dans quel sens varie la quantité monétisée q lorsqu'un des facteurs clés change. En revanche, nous ne pouvons pas, à ce stade, donner une échelle de grandeur à l'effet que produit chacun de ces facteurs sur les quantités monétisées, ni même dire lequel de ces facteurs a une plus grande influence sur la quantité q que les autres. Or, il est important de faire cet exercice si nous voulons établir une échelle de priorité dans le choix des actions à entreprendre pour lutter contre la monétisation. Pour ce faire, nous avons choisi d'utiliser la fonctionnalité de contribution à la variance que nous offre le logiciel @RISK de Palissade. Cette fonctionnalité permet de superposer sur le même graphique les grandeurs et la direction de chaque facteur d'entrée et de voir celui qui produit le plus d'effet sur q.

j) Contribution de chaque facteur exogène à la variance

Les résultats de la contribution à la variance confirment le sens des variations représenté dans le tableau 6.3. La commission (w), le prix (a) du renseignement et les contremesures (béta) varient dans le même sens, celui des contraintes budgétaires et de contremesures telles qu'énoncées au paragraphe 5.1. Quant à R, le revenu anticipé, il évolue dans le sens contraire, constituant ainsi la principale motivation extrinsèque du fraudeur risquophobe (cf. figure 6.7).

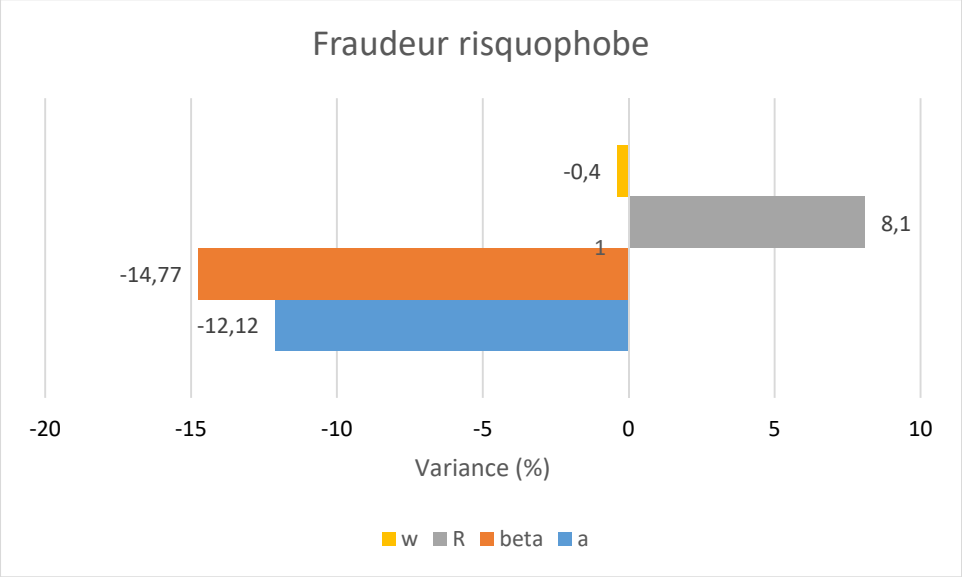


Figure 6.7 : Intensité et direction de l'effet de chaque facteur clé sur la quantité monétisée q

Pour le fraudeur risquophile (cf. figure 6.8), son appétit plus accru pour l'argent explique toute l'importance de R, laquelle importance se traduit ici par l'amplitude de ce facteur qui est plus élevée que celle du même facteur pour le fraudeur risquophobe. Quant aux intensités des contraintes w et beta, elles sont, à quelques chiffres près, semblables à ce que nous avons obtenu avec le fraudeur risquophobe. Aussi, la probabilité de se faire arrêter semble croître avec q. Toutefois, son intensité est négligeable.

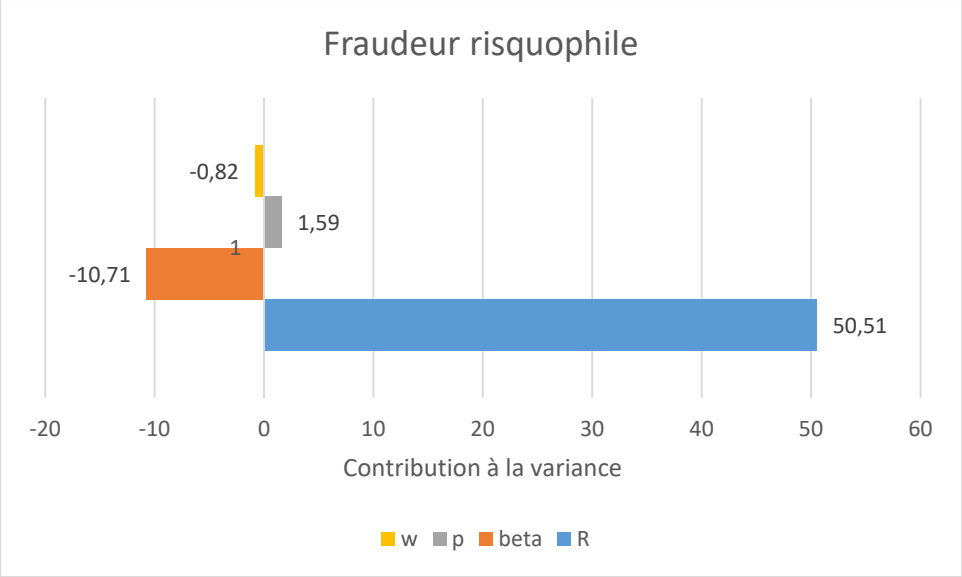


Figure 6.8 : Intensité et direction de l'effet de chaque facteur clé sur la quantité monétisée q

À la lumière de la statique comparative que nous venons de faire, il se dégage un certain nombre de liens potentiels entre certains facteurs exogènes clés de notre modèle et les quantités que le fraudeur peut monétiser, eu égard à sa fonction d'utilité. Par exemple, nous avons montré que le revenu anticipé et la richesse initiale du fraudeur risquophobe ont des effets positifs sur les quantités monétisées, toutes choses égales par ailleurs. Mais, nous n'avons pas étudié l'effet que produirait la variation simultanée (comme dans la vie réelle) de ces mêmes facteurs sur la variable endogène lorsque l'ensemble du mouvement tend vers un état d'équilibre. C'est ce que permet de faire une simulation de Monté Carlo. Cette simulation est d'autant plus appropriée dans notre contexte car c'est un système complexe – six paramètres -, un système au sujet duquel nous ne disposons pas d'informations précises sur ces facteurs et pour lequel il n'existe pas, à notre connaissance, de solution analytique.

6.10 Simulation de Monte Carlo

Avant de présenter nos résultats de simulation, rappelons que notre postulat est à l'effet que les variables d'entrée du modèle, c'est-à-dire les facteurs clés de monétisation, suivent une loi de distribution triangulaire. Nous avons défini les valeurs minimum, probable et maximum (cf. paragraphe 6.8 : Données de simulation).

La courbe en *S* de la figure 6.9 qui résulte de cette simulation présente la probabilité d'occurrence de monétisation en fonction du cumul des quantités q. En examinant l'étalement de q et la probabilité d'occurrence inhérente, on observe que le fraudeur risquophobe a un étalement restreint avec une probabilité élevée. Ce qui peut être interprété comme une attitude prudente. Le fraudeur risquophobe préfère monétiser des renseignements de «qualité» et vite car ces renseignements ont plus de chance d'être convertis que ceux de moins bonne qualité.

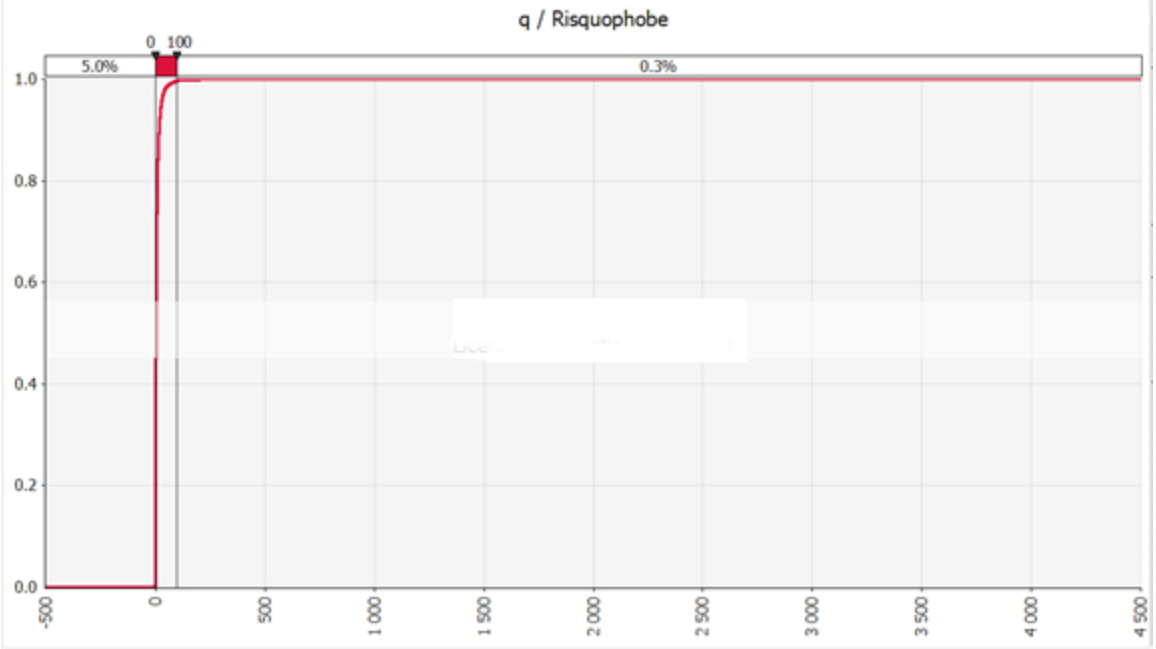


Figure 6.9 : Fréquence cumulative des quantités monétisées

En revanche, la plage des quantités q du fraudeur risquophile est plus étalée et la probabilité moins élevée, représentant ainsi une plus grande espérance de monétisation que la distribution de la figure 6.10. Le fraudeur qui aime le risque tentera de monétiser plus des renseignements sans autant d'égards à la qualité qu'un risquophobe puisqu'il est plus enclin à prendre de risque et à vouloir faire plus d'argent.

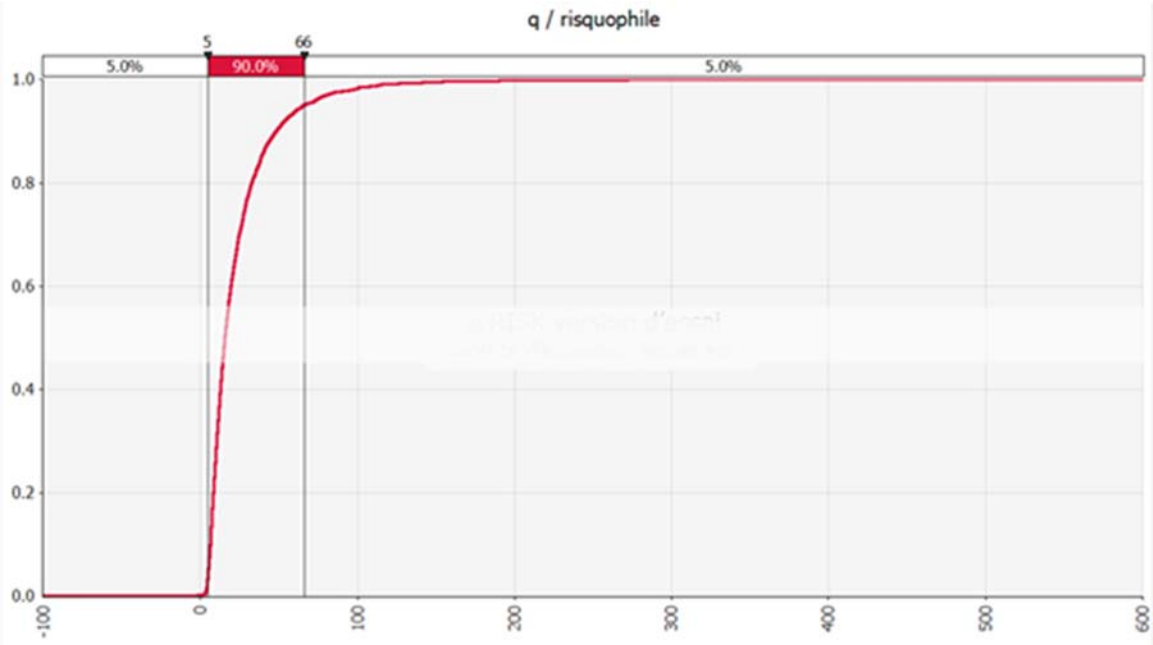


Figure 6.10 : Fréquence cumulative des quantités monétisées pour un fraudeur «risquophile»

Les figures 6.11 et 6.12 ci-dessous représentent les plages et les distributions des résultats de q susceptibles de se produire lorsque l'on fait varier tous les facteurs exogènes simultanément (comme dans la vie réelle). On s'aperçoit qu'après 100 itérations, il n'y a pas convergence de valeurs de q. L'équilibre entre, d'un côté, l'intensité de motivation due au revenu anticipé et, de l'autre, les obstacles que représentent le niveau de sécurité et les charges de monétisation (prix, commissions) n'est donc pas assuré dans cet intervalle.

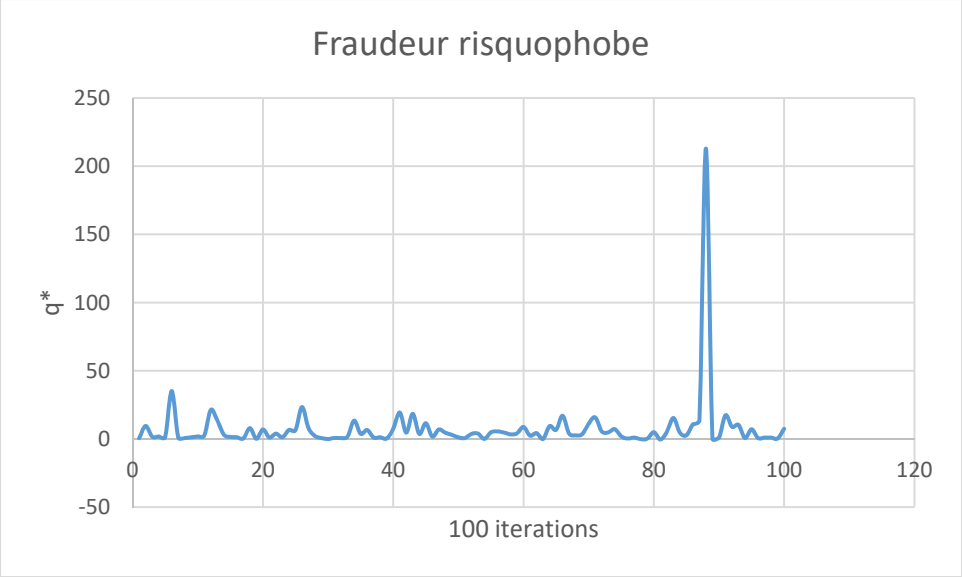


Figure 6.11 : Variation des quantités monétisées q lorsque l'on tend vers l'équilibre

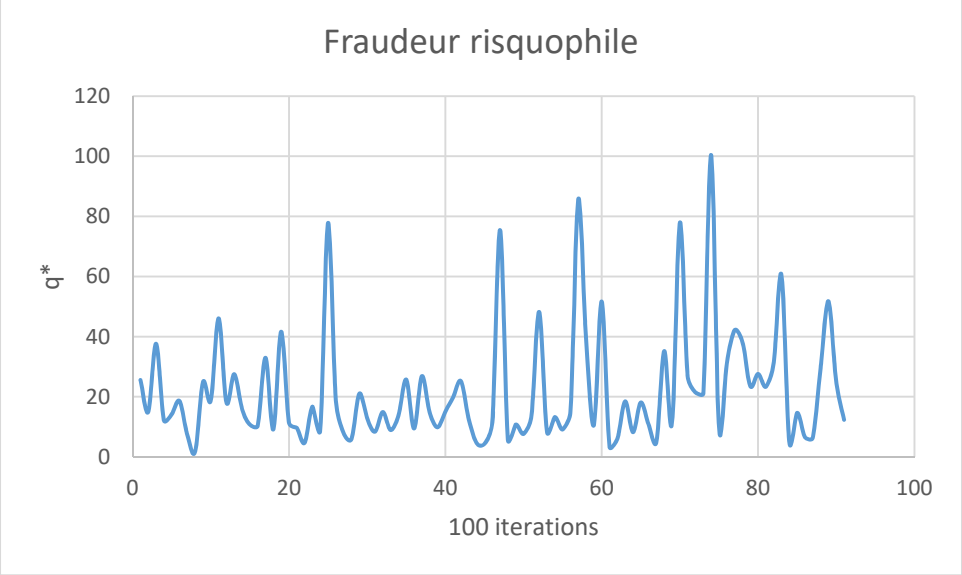


Figure 6.12 : Variation des quantités monétisées q lorsque l'on tend vers l'équilibre.

On obtient des résultats similaires après 1000 itérations (cf. figure 13 et 14). Ce qui veut dire que nous n'avons pas trouvé de combinaisons de valeurs des facteurs exogènes qui assurent au fraudeur une quantité q positive. Il n'y a donc pas d'équilibre dans cette partie du marché noir de la

monétisation. En revanche, notre modèle met en lumière les conditions, à minima, pour un équilibre partiel. Ces conditions prennent la forme d'un système de trois équations à trois inconnus : revenus anticipés du fraudeur, charges de monétisation (commission de la mule, prix du renseignement, etc.) et niveau de sécurité. Un système pour lequel nous ne disposons pas de données précises pour élaborer des solutions.

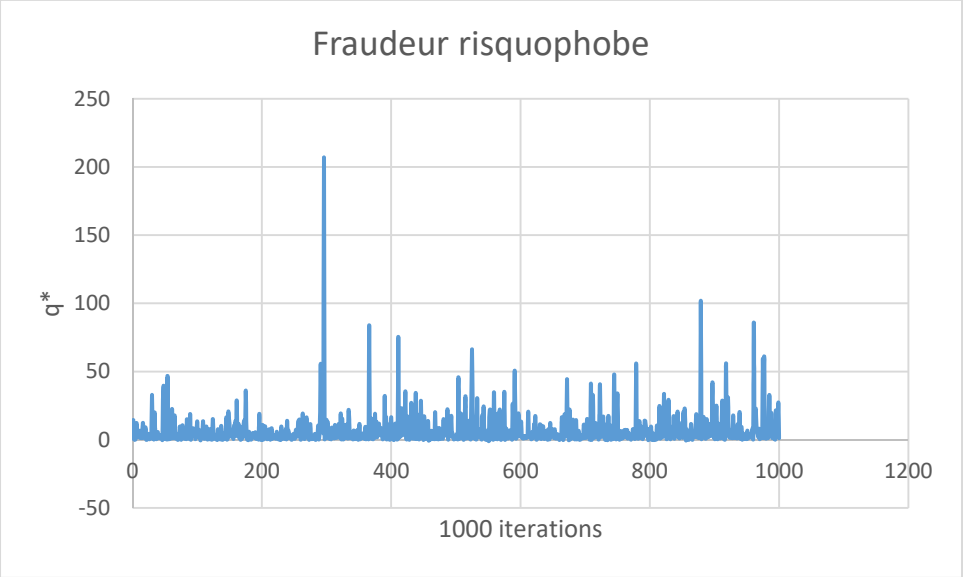


Figure 6.13 : Variation des quantités monétisées q

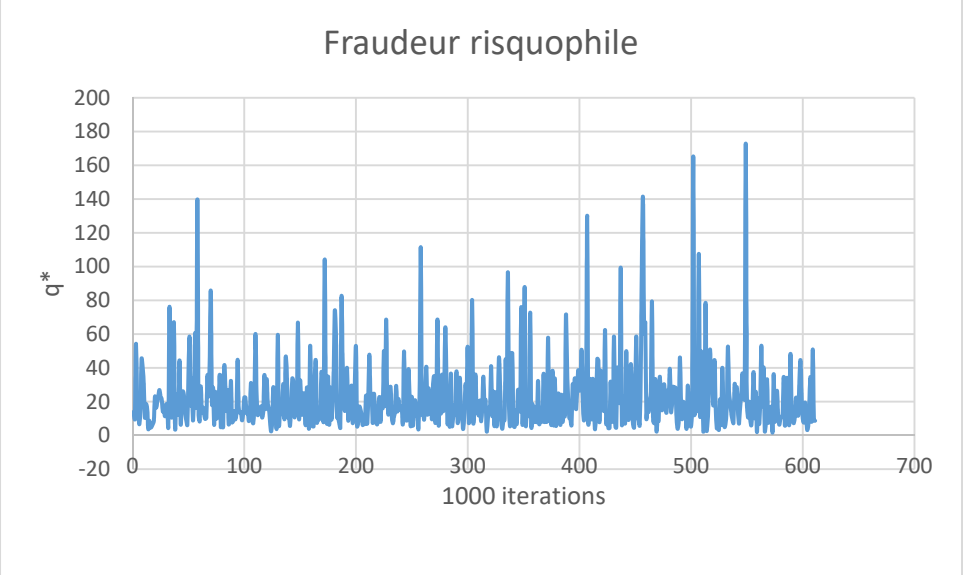


Figure 6.14 : Variation des quantités monétisées q

6.11 Discussion

Le premier résultat qui émane de ce modèle est sans aucun doute la confirmation que le revenu anticipé, le niveau de sécurité issu des contremesures mises en place par les banques et les commissions versées à la mule sont les trois facteurs clés qui ont un plus grand impact sur la monétisation, très loin devant la probabilité de se faire prendre, la richesse initiale et le prix du renseignement. Ce résultat est, au regard de la littérature consultée, prévisible. Ce qui l'est moins, c'est l'intensité et le sens de variation des effets de ces facteurs exogènes. Ces effets, nous les avons estimés par simulation (cf. Tableau 6.3) et, à notre grande surprise, le prix du renseignement et la richesse initiale ont des résultats en partie contre-intuitifs. Nous pouvons attribuer cette situation à une seule et même raison : la fonction d'utilité du fraudeur. Dans le cas du fraudeur risquophobe, il évalue ce qu'il perd - et non ce qu'il gagne - s'il achète des renseignements à des prix élevés. Et, en ce sens, son appréhension d'un prix de renseignement élevé devient un frein à sa motivation et par le fait même réduit ses chances de monétiser. En revanche, le fraudeur risquophile, lui, préfère miser toute sa richesse malgré une espérance de gain négative. La richesse initiale n'a donc pas d'effet sur la quantité qu'il peut monétiser.

Le second résultat concerne les mêmes facteurs clés de la monétisation mais vus à travers le prisme de l'équilibre du marché. Certains de ces facteurs constituent des charges pour le fraudeur et d'autres, des revenus anticipés. Une baisse de l'intensité des revenus anticipés –cas du fraudeur risquophobe- entraîne une diminution de la motivation principale –même si les charges sont basses- et donc une baisse probable des quantités monétisées. En revanche, un accroissement de l'intensité des revenus anticipés – cas du fraudeur risquophile - n'augmente pas forcément les chances de monétiser. Il n'est donc pas possible d'envisager un équilibre dans ce type d'activités car plusieurs autres éléments non modélisables rentrent en ligne de compte. Le premier élément est la réversibilité des transactions bancaires. En effet, le fait que les transactions bancaires ordinaires soient réversibles a comme effet que lorsque la fraude est découverte, la transaction est annulée et le fraudeur repéré (Cárdenas et al., 2010; Herley, 2014). Conséquence, les renseignements achetés dans ce marché ne sont pas facilement convertibles en argent, sauf si le fraudeur utilise les services d'un passeur ou mule qui se charge de blanchir les renseignements en acceptant des transferts réversibles à partir d'un compte compromis et en procédant aux transferts irréversibles (comme par Western Union). Un risque que très peu de gens peuvent accepter.

Le second élément est la qualité du renseignement. En supposant que la mule soit disponible et efficace, un autre facteur important qui contribue à favoriser /défavoriser la monétisation est ce que nous qualifions dans ce texte de « qualité du renseignement ». On entend par qualité du renseignement, l'effet combinée de l'origine et du type du renseignement, des options qu'il offre (platine, or, etc.) de sa durée sur le marché, du solde disponible, du code de sécurité et des informations personnelles du détenteur(quotidien, 2013).

Enfin, il y a l'asymétrie de l'offre dans ce marché qui n'arrange pas les choses pour le fraudeur. À titre d'exemple, on retrouve plus de « cartes américaines en circulation que de cartes européennes, notamment à cause des nombreux piratages de bases de données d'entreprises américaines. Or, ce qui est rare est cher. Par conséquent, les cartes bancaires européennes, moins nombreuses, ont plus de valeur (quotidien, 2013)».

Pour toutes ces raisons, il serait très imprudent de prédire la quantité de renseignements monétisés à partir des facteurs que nous venons d'étudier. L'équilibre dans l'activité de monétisation étant très difficile à atteindre. Nos résultats de simulation le montrent bien. Nous pensons quand même qu'on pourrait s'en approcher si l'on dispose des données réelles.

6.12 Conclusion

Dans ce chapitre, nous avons présenté un modèle microéconomique d'équilibre partiel qui analyse le comportement du fraudeur au cours de l'activité de monétisation des renseignements volés par hameçonnage. Nous avons étudié plusieurs hypothèses relatives à plusieurs facteurs exogènes que nous avons définis et à la fonction d'utilité du fraudeur.

Il appert que six variables influent sur les quantités de renseignements monétisées. Il y a le revenu anticipé, l'intensité du niveau de sécurité, la commission versée à la mule, le prix du renseignement, la richesse initiale du fraudeur et la probabilité de se faire arrêter. Parmi ces facteurs, la commission versée à la mule, l'intensité du niveau de sécurité et le prix d'achat du renseignement ont un effet négatif sur les quantités monétisées (q) alors que le revenu anticipé du fraudeur et la probabilité de se faire arrêter sont deux fonctions croissantes de q.

Les résultats de simulation confirment donc nos trois premières hypothèses, à l'effet que :

- la quantité monétisée q est une fonction croissante de la probabilité de se faire arrêter (H6.1);

- l'augmentation du revenu anticipé a un effet positif sur la quantité monétisée (H6.2);
- l'accroissement des contremesures réduit les chances de monétiser (H6.3).

En revanche, l'hypothèse (H6.4) selon laquelle la quantité monétisée q est une fonction croissante de la commission versée à la mule n'est pas confirmée. C'est plutôt le contraire qui semble se produire. C'est-à-dire que plus la commission est attrayante, plus élevé est le risque de se faire prendre et moins grandes sont les chances de monétiser.

Aussi, le choix des fonctions d'utilité de types CARA ou CRRA ne modifie en rien le sens des effets du revenu anticipé, des contremesures et de la probabilité sur le risque de monétisation, leurs impacts se situant plutôt au niveau de l'amplitude de ces effets (Cf. Figure 6.).

Quant aux hypothèses H6.5 et H6.6, elles réfèrent toutes les deux à la même ressource : la capacité (cf. paragraphe 6.7.6). La décision du fraudeur est dans ce contexte guidée par les mêmes considérations que tout agent économique rationnel. Il compare le prix (coût) et sa richesse initiale et son attitude face au risque est caractérisée par la fonction d'utilité du fraudeur (CARA ou CRRA).

Relativement aux effets simultanés des variables exogènes sur la quantité monétisée, notre modèle montre qu'il n'existe pas de vecteurs de valeurs qui assurent un équilibre dans l'activité de monétisation. Les raisons qui expliquent cette absence d'équilibre dans ce secteur du marché constituent une piste de recherche pour les travaux futurs.

En terminant, soulignons que notre recherche a le mérite de définir le nombre, l'amplitude et le sens de variation des inconnus du système d'équation de la monétisation et de poser certaines conditions de sa résolution. Et, bien que ce modèle soit théorique et que les résultats soient à prendre avec prudence, il révèle à tout le moins, l'importance de la fonction d'utilité du fraudeur dans ce processus de monétisation. Nous pensons qu'une analyse plus approfondie de l'influence de ce facteur permettrait de mieux comprendre le comportement du fraudeur dans cette partie du marché noir des renseignements.

À la lumière de ce qui précède, le second bloc de l'approche de réduction de risque que nous proposons dans cette thèse est complété comme le montre la Figure 6.15 ci-dessous.

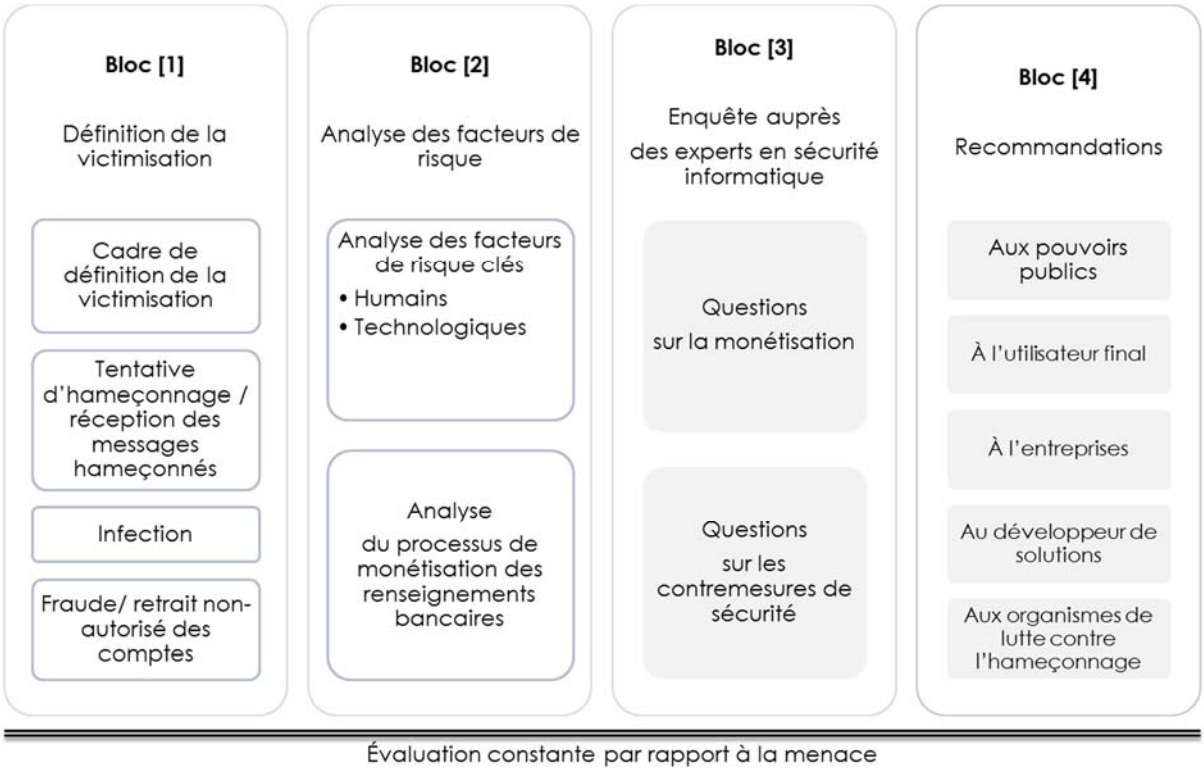


Figure 6.15 : Approche de réduction de risque d'hameçonnage bancaire proposée

CHAPITRE 7 RÉSULTATS DE L'ENQUÊTE AUPRÈS D'EXPERTS

Au chapitre deux, consacré à la revue de littérature, nous avons relevé des insuffisances de certaines mesures de lutte contre l'hameçonnage bancaire. Ensuite, nous avons recueilli auprès des experts en sécurité informatique leurs opinions sur ces insuffisances et les suggestions d'amélioration qu'ils proposent pour les corriger.

Ce chapitre présente les résultats de cette enquête. Il est organisé comme suit : la première section est consacrée aux résultats détaillés, la deuxième donne une interprétation des résultats, la troisième fait la synthèse et elle est suivie de la discussion ainsi que de la conclusion.

7.1 Résultats détaillés

Nous avons choisi de les présenter selon la séquence des énoncés du questionnaire d'enquête.

7.1.1 Monétisation

Dans la partie A du questionnaire de l'enquête, les répondants ont été invités à évaluer leur degré d'accord avec neuf énoncés qui résument les principaux facteurs qui influencent le processus de monétisation dans un marché noir et que nous avons identifiés dans la revue de la littérature.

Globalement, plus de 50% des répondants ont confirmé que six des neuf facteurs de monétisation identifiés dans la revue de littérature ont une influence au moins forte sur le processus de monétisation d'un renseignement. Ces facteurs sont : le revenu anticipé, la qualité de renseignements achetés au marché noir, le temps que chaque renseignement a mis sur le marché, le niveau des contremesures opérationnelles mises en place par les banques, le fait d'agir sous anonymat et le prix du renseignement.

Relativement au revenu anticipé, le degré d'accord à l'effet que son influence est élevée voire très élevée sur la monétisation est de près 88%. L'anonymat arrive en second rang dans l'opinion des experts avec un taux d'accord de près de 81%, suivi, dans l'ordre, de la qualité du renseignement (75%), du prix du renseignement (73%), du temps écoulé depuis que le renseignement est sur le marché (66%) et du niveau des contremesures mises en place par les banques (50%).

Les autres facteurs comme la commission versée à la mule, la probabilité de se faire arrêter et la richesse initiale du fraudeur ont été les plus bas avec des scores compris entre 12 et 23%. Les résultats exhaustifs de l'évaluation des experts pour cette partie A du questionnaire sont présentés à l'annexe J et au Tableau K.6. Nous reviendrons sur ces résultats au chapitre 8 afin de les comparer aux résultats obtenus de la simulation de notre modèle théorique.

7.1.2 Contremesures de sécurité

Dans la première section de la partie B du questionnaire de l'enquête, cinq catégories de contremesures ont été identifiées par la revue de littérature comme devant être améliorées afin de réduire le risque. Il s'agit :

1. des filtres anti-hameçonnage;
2. des navigateurs et des modules de gestion des mots de passe;
3. des listes de restriction et des fichiers de journalisation;
4. de la sécurisation de l'information lors de transactions bancaires en ligne;
5. des formations et les campagnes de sensibilisation aux enjeux de sécurité.

7.1.2.1 Filtres anti-hameçonnage : suggestions d'améliorations des experts

Relativement aux filtres anti-hameçonnage, nous avons demandé aux experts de classer par ordre d'efficacité cinq énoncés de mesures d'améliorations de réduction des taux d'erreurs (faux positifs, faux négatifs). Le tableau 7.1 ci-dessous résume le choix des experts. On y remarque que les avis des experts sur le mécanisme d'empreinte avec authentification de l'émetteur pour réduire le taux d'erreurs des filtres anti-hameçon est privilégié si l'on additionne les degrés d'influence forte et très forte. Ce facteur est suivi de la campagne de sensibilisation continue aux enjeux de sécurité, de la formation de base en sécurité et de la signature numérique qui arrivent à ex aequo dans l'opinion des experts avec 59% des réponses favorables. L'amélioration des critères de rejet arrive en dernier. Les résultats détaillés sont présentés au Tableau K.1. Nous reviendrons sur ce résultat au chapitre 8 lors de la discussion sur l'approche globale de réduction de risque que nous proposons.

Tableau 7.1 : Classement des mesures d'améliorations des filtres anti-hameçon

	Meilleur réglage des critères de rejet	Signature numérique	Mécanismes d'empreinte avec authentification de l'émetteur	Formation de base en sécurité	Campagne de sensibilisation continue aux enjeux de sécurité
Total répondants / Échelle d'influence	N=17	N=17	N=16	N=17	N=17
Très faible	24%	12%	6%	6%	0%
Faible	18%	6%	6%	29%	24%
Moyen	29%	24%	25%	6%	18%
Forte	18%	35%	38%	18%	6%
Très forte	12%	24%	25%	41%	53%

Nous avons aussi demandé aux experts de proposer d'autres mesures ou, à tout le moins, de suggérer des améliorations à apporter aux mesures existantes. En réponse à cette question, les trois suggestions d'améliorations les plus communes suivantes ont été faites :

1. L'amélioration des mécanismes de «Machine Learning» dans les filtres : six experts sur sept (85%) ayant répondu à cette question ont suggéré que des améliorations soient apportées aux mécanismes d'apprentissage automatique. Selon ces experts, ces améliorations permettraient d'adapter les analyses que font les filtres en se fondant sur l'analyse de données empiriques provenant d'une base de données comportementales.
2. Une bonne implémentation de la cryptographie dans la signature numérique et dans les mécanismes d'empreinte avec authentification de l'émetteur.
3. Le renforcement des méthodes d'authentification par rajout de questions.

7.1.2.2 Navigateurs et des modules de gestion des mots de passe

Au niveau des navigateurs, la revue de littérature a révélé que la variété des barres de gestion des navigateurs et des modules de gestion des mots de passe pouvait semer de la confusion dans l'esprit des utilisateurs et créer un risque de victimisation inhérent à une mauvaise utilisation. Dans la seconde section de la partie B du questionnaire, il est proposé six énoncés de mesures à prendre pour pallier ce risque. Les avis des experts privilégient, à plus de 82%, deux mesures : l'intégration de l'authentification multifactorielle dans les navigateurs et l'intégration d'un système d'alerte

anti-hameçonnage dans les navigateurs. L'activation du certificat EV SSL à validation étendue dans le navigateur arrive en troisième position avec plus de 53% des avis des experts.

Les autres mesures recueillent chacune moins de 42% des avis des experts.

Tableau 7.2 : Classement des mesures d'amélioration des navigateurs

	Mise en place d'une barre d'outils standard pour les navigateurs	Mise en place d'un module standard de gestion des mots de passe	Adoption d'un navigateur standard pour toute l'organisation	Systèmes d'alerte anti-phishing actifs (intégrés) dans les navigateurs	Certificat EV SSL à validation étendue	Authentification multifactorielle
Total répondants / Échelle d'influence	N=16	N=17	N=17	N=16	N=17	N=17
Très faible	19%	6%	29%	0%	6%	0%
Faible	31%	24%	24%	6%	12%	6%
Moyen	25%	29%	29%	13%	29%	12%
Forte	25%	29%	12%	69%	35%	12%
Très forte	0%	12%	6%	13%	18%	71%

De même que pour la question précédente, les experts ont été amenés à suggérer d'autres améliorations à apporter aux mécanismes anti-phishing offerts dans les navigateurs actuels.

C'est ainsi qu'on retrouve dans l'ordre :

1. L'élimination de certaines options sur les navigateurs, notamment :
    a. l'option de remplissage automatique des formulaires ;
    b. la sauvegarde des mots de passe ;
    c. l'option de persistance des sessions dans les navigateurs.
2. L'amélioration des méthodes de détection (ex. détection des attaques bitsquatting).
3. Mise à jour régulière des applications Internet riches (RIA pour Rich Internet Application, également connues comme des applets ou applications Web Start).

7.1.2.3 Listes de restriction et fichiers de journalisation

Dans la troisième section de la partie B du questionnaire, nous avons demandé aux experts, à travers cinq énoncés, d'exprimer leur degré de satisfaction à l'égard des délais de mise à jour des listes de restriction et de fichiers de journalisation et de proposer, le cas échéant, d'autres mesures qu'ils jugent efficaces pour réduire ces délais.

Moins de 43% des experts ont déclaré un niveau élevé (fort) et très élevé (très fort) de satisfaction à l'égard du temps moyen de mise à jour des listes noires. La satisfaction à l'égard des autres énoncés étant bien en dessous de ce chiffre (cf. Tableau 7.3), le problème des délais de mise à jour des listes noires et des fichiers de journalisation semble être bien réel car les avis des experts sondés confirment les résultats de la majorité des travaux antérieurs que nous avons consultés sur ce sujet.

Tableau 7.3 : Classement des mesures d'amélioration des listes de restriction

	degré de satisfaction à l'égard du temps moyen de mise à jour de listes noires	degré de satisfaction à l'égard du temps moyen de mise à jour de fichier de journalisation au Canada	degré de satisfaction à l'égard du temps moyen de mise à jour de fichier de journali-sation à l'étranger	votre degré de satisfaction à l'égard de la collaboration entre les partenaires - police	votre degré de satisfaction à l'égard de la collabo-ration entre pays
Total répondants / Échelle d'influence	N=14	N=9	N=9	N=10	N=11
Très faible	7%	0%	11%	30%	45%
Faible	21%	22%	22%	40%	36%
Moyen	29%	44%	33%	20%	9%
Forte	36%	22%	22%	10%	9%
Très forte	7%	11%	11%	0%	0%

Nous avons voulu savoir ce que pensent ces experts de l'idée de corriger ce problème par une solution juridique contraignante relative à l'échange des informations nécessaires à la mise à jour des listes de restrictions. 84% des experts pensent que cette mesure contribuerait efficacement voire très efficacement à réduire les délais de mise à jour de ces listes de restriction (cf. Tableau K.3). Parmi ces experts, six vont plus loin et suggèrent :

- un modèle commun pour assurer le partage des informations rapidement ;
- la détermination d'une autorité commune pour s'assurer de la mise en place de cette solution (ex. Une liste noire au niveau provincial) ;
- la détermination d'un standard de publication ;
- un incitatif pour les usagers – renforcement positif-.

7.1.2.4 Sécurisation de l'information lors de transactions bancaires en ligne

Dans cette section de l'enquête, les experts ont été invités à évaluer leur niveau d'accord avec quatre énoncés de mesures pour améliorer la sécurisation de l'information lors des transactions bancaires et qui ont été présentés dans la revue de la littérature : le chiffrement

des transactions, l'authentification des transactions en ligne par les protocoles 3D-Secure ou «Verified By» de Visa et l'utilisation des témoins et de la signature numérique. La majorité des répondants (69%) ont affirmé que le chiffrement des transactions est efficace voire très efficace pour sécuriser les transactions en ligne devant l'authentification par 3D-Secure ou «Verified By» de Visa (56%) qui, elle, est suivie de la signature numérique avec 53% des voix. Les témoins ou log de suivi des sessions arrivent en dernier comme on peut le remarquer dans le tableau 7.4 ci-dessous.

Tableau 7.4 : Classement des mesures d'amélioration pour la sécurisation des transactions

	Chiffrement des transactions	Témoins	Authentification de transaction en ligne par des protocoles suivants	Signature numérique
Total répondants / Échelle d'influence	N=16	N=16	N=16	N=15
Très faible	6%	13%	6%	7%
Faible	6%	25%	6%	20%
Moyen	19%	31%	31%	20%
Forte	25%	19%	50%	33%
Très forte	44%	13%	6%	20%

Parmi les autres mesures suggérées par les experts, notons :

- l'authentification multifactorielle (ex. 3e facteur, code via SMS);
- l'utilisation des questions de sécurité;
- la géolocalisation de l'utilisateur via son IP;
- la sensibilisation personnelle;
- la théorie du Nudge (Économie comportementale).

7.1.2.5 Formations et campagnes de sensibilisation sur les enjeux de sécurité

La dernière section de la partie B du questionnaire comprend quatre énoncés en lien avec le degré de satisfaction des experts à l'égard des formations et campagnes de sensibilisation

aux enjeux de sécurité. C'est par une forte majorité, plus de 70%, que les experts ont exprimé leur insatisfaction à l'égard de l'ensemble des quatre énoncés pour lesquels ils se sont prononcés (cf. tableau 7.5 ci-dessous).

Ce qu'on apprend à travers ce résultat, c'est que les experts sont très peu satisfaits de l'utilisation qu'on fait ou qu'on ne fait pas des réseaux sociaux (à peine 6%) pour mener des campagnes grand-public de sensibilisation aux enjeux de sécurité. Ces chiffres nous indiquent aussi qu'il y a une forte proportion de réponses ni «en accord», ni «en désaccord» (40%) sur la satisfaction par rapport au développement des outils de formation pour accompagner les utilisations. Nous reviendrons sur ce taux élevé d'indécision.

Tableau 7.5 : Classement des mesures d'amélioration pour la formation et la sensibilisation aux enjeux de sécurité

	Degré de satisfaction à l'égard de la formation anti-phishing individuelle	Degré de satisfaction à l'égard de la formation anti-phishing de groupe	Degré de satisfaction à l'égard des campagnes grand-public utilisant les réseaux sociaux	Degré de satisfaction à l'égard des développements des outils de formation
Total répondants / Échelle d'influence	N=15	N=16	N=17	N=15
Très faible	13%	19%	35%	7%
Faible	27%	31%	41%	33%
Moyen	27%	31%	18%	40%
Forte	27%	19%	6%	13%
Très forte	7%	0%	0%	7%

Parmi les autres mesures suggérées par les experts, on retrouve :

- formation/campagne (publicité gouvernementale à grande échelle);
- formation des jeunes (dès leur première utilisation d'un ordinateur);
- rendre obligatoires via des lois les séances de sensibilisation et de formation;
- publier des vidéos sur la page personnelle des clients;

- sensibiliser les clients lors des ouvertures de compte bancaire, clip sur sites bancaires;
- incitatifs financiers;
- formation et sensibilisation de façon continue;
- publicité plus choc afin de sensibiliser davantage les gens;
- guide d'information pour les nouveaux arrivants dans les entreprises;
- ludification[66] (gamification en anglais - utilisation des jeux).

7.2 Interprétation des résultats de l'enquête

Sur la base des résultats détaillés que nous venons de présenter, nous pouvons regrouper en trois grandes catégories les réponses des experts : il y a la catégorie pour laquelle les réponses des experts sont défavorables aux énoncés des questions (choix de réponse : très faible et faible), il y a celle pour laquelle les réponses des experts y sont favorables (choix de réponse : très fort et fort) et celle pour laquelle les réponses aux énoncés ne sont ni favorables ni défavorables. Nous nous intéressons dans le reste du chapitre aux deux dernières catégories, la première catégorie étant écartée pour la raison que les énoncés ont été majoritairement rejetés par les experts.

Pour la catégorie où le choix des réponses aux énoncés n'est ni favorable ni défavorable, nous observons que les scores sont assez élevés pour certaines mesures. Par exemple, 40% des répondants ne se déclarent ni satisfaits, ni insatisfaits à l'égard des développements des outils de formation. Il en est de même pour le degré de satisfaction ou d'insatisfaction à l'égard du temps moyen de mise à jour de fichier de journalisation au Canada où 44% des répondants ne sont ni en désaccord, ni en accord. Nous avons regroupé dans le Tableau 7.6 ci-dessous quelques-uns des énoncés pour lesquels le taux d'indécision est supérieur à un seuil que nous nous sommes fixés, soit de 25 %.

---

[66] C'est l'utilisation des mécanismes de jeu dans le développement des sites web, des applications d'apprentissage, des réseaux sociaux avec pour objectif d'augmenter leur acceptabilité et leur utilisation.

Tableau 7.6 : Réponses ni favorables ni défavorables

#	Énoncé de l'enquête	# répondants	% des experts ni en désaccord, ni en accord (moyen)
1.	Richesse	N=16	50%
2.	Commission	N=15	47%
3.	Degré de satisfaction à l'égard du temps moyen de mise à jour de fichier de journalisation au Canada	N=9	44%
4.	Degré de satisfaction à l'égard des développements des outils de formation	N=15	40%
5.	Degré de satisfaction à l'égard du temps moyen de mise à jour de fichier de journalisation à l'étranger	N=9	33%
6.	Niveaux des contremesures mises en place par les banques	N=16	31%
7.	Authentification de transaction en ligne par des protocoles 3D-Secure ou Verified By Visa et MasterCard SecureCode	N=16	31%
8.	Témoins[67]	N=16	31%
9.	Meilleur réglage des critères de rejet	N=17	29%
10.	Adoption d'un navigateur standard pour toute l'organisation	N=17	29%
11.	Mise en place d'un module standard de gestion des mots de passe	N=17	29%
12.	Degré de satisfaction à l'égard du temps moyen de mise à jour de listes noires	N=14	29%
13.	Mécanismes d'empreinte avec authentification de l'émetteur	N=16	25%
14.	Mise en place d'une barre d'outils standard pour les navigateurs	N=16	25%

On y observe, par exemple, que l'énoncé sur le facteur de richesse du fraudeur obtient le plus haut taux de choix de réponse «moyen» (50%). Ce qui veut dire que la moitié des experts qui ont répondu à la question considère que la richesse initiale du fraudeur contribue moyennement à la monétisation des renseignements bancaires.

[67] C'est un fichier contenant des éléments d'information que le site Web de la banque crée automatiquement lorsqu'un client le visite. Par exemple, lorsqu'un client se connecte à «service Net» d'une banque, le serveur du «service Net» capture ces informations et pendant toute la durée de la session d'utilisation, il fait les vérifications nécessaires pour s'assurer que la banque fait affaire avec le bon client.

En raison de la taille restreinte de notre échantillon, nous pensons qu'un tel résultat nécessite qu'on investigue davantage afin de prendre en compte, si tel devrait être le cas, tout éventuel biais dans les réponses des experts.

Pour cela, nous avons émis trois conjectures. Nous pensons que la réponse de l'expert est mitigée soit parce que la mesure présente des insuffisances pour garantir une meilleure efficacité dans la lutte contre l'hameçonnage, soit parce que la question n'est pas suffisamment claire, ou encore parce qu'il y a des variations importantes dans l'appréciation que font ces experts de l'énoncé. En ce sens, il serait important de s'interroger sur les facteurs qui peuvent avoir influencé les experts dans leur choix de réponse. L'idée étant de vérifier si ce résultat est le choix de la majorité, auquel cas ce serait considéré comme un genre de consensus chez ces experts, ou alors, s'il existe des différences entre les réponses de ces experts. Pour ce faire, nous avons réalisé une analyse de la variance (ANOVA à un facteur) afin de déterminer s'il existe des liens entre le nombre d'années d'expérience et le choix de l'expert pour les énoncés ci-dessus et pour lesquels la proportion des experts qui ont répondu «moyen» nous semble élevée.

7.2.1 L'impact de l'expérience sur les choix des experts

Dans la première page du questionnaire de l'enquête, des questions d'ordre général ont été posées aux participants. Parmi ces questions, une en particulier visait à déterminer le profil du participant eu égard à son expérience en sécurité informatique et dans la lutte contre l'hameçonnage. La métrique utilisée pour mesurer cette expérience est le nombre d'années. Pour ce qui est des autres questions de la même rubrique, nous n'avons pas pu les exploiter car les réponses étaient, soit très vagues, soit trop spécifiques et ne permettent pas de s'en servir pour différencier les répondants.

a) Expérience des experts

Pour la suite de l'analyse, nous avons défini quatre groupes d'experts selon le nombre d'années d'expérience en sécurité informatique ou en hameçonnage. La Figure 7.1 qui suit présente ces groupes. Nous utilisons ces groupes dans notre analyse de la variance afin de tenter d'expliquer la raison pour laquelle il y a une si forte proportion d'experts qui aient choisi moyen pour plusieurs énoncés.

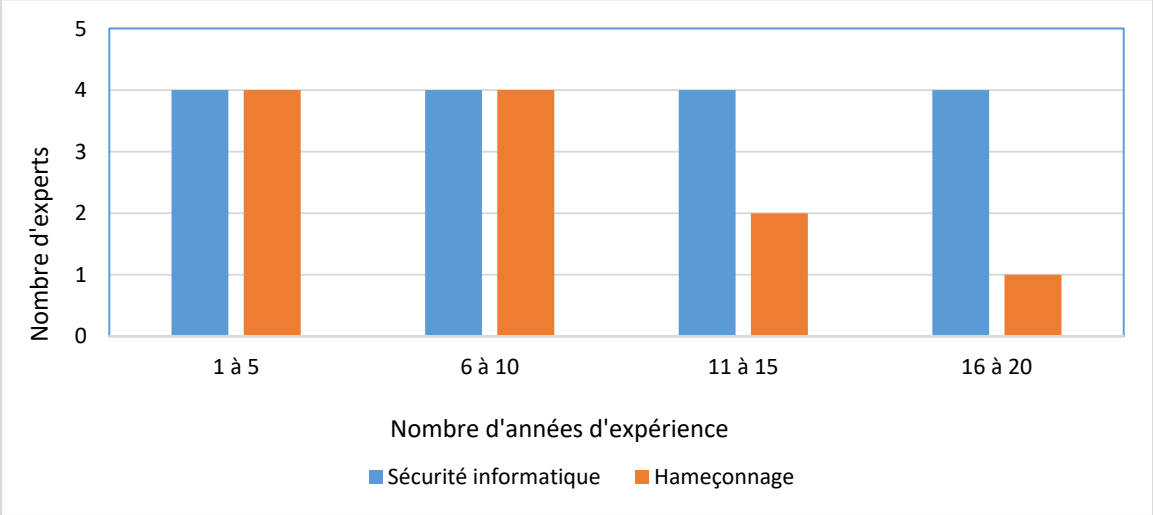


Figure 7.1 : Répartition des experts selon l'expérience

b) Analyse de la variance

Un extrait des résultats de cette analyse est présenté dans le Tableau 7.7 ci-dessous. On y observe que la valeur de F[68] est très grande (F>1), à la fois, pour l'expérience en hameçonnage et pour l'expérience en sécurité informatique. Ces résultats laissent suggérer qu'il existe une différence importante entre la moyenne des choix des quatre groupes d'experts si l'on considère le nombre d'années d'expérience en sécurité informatique et en hameçonnage pour trois des quatorze énoncés pour lesquels la proportion des experts qui ont répondu «moyen» nous semble élevé. Le niveau de signification statistique étant inférieur à 0,05 pour chacun de ces trois énoncés, on peut donc conclure que le nombre d'années d'expérience en hameçonnage semble avoir eu une incidence dans le choix de l'ordre d'efficacité de deux des trois énoncés présentés au tableau 7.7, notamment :

- un meilleur réglage des critères de rejet contribue efficacement à la réduction des taux d'erreurs (faux positifs, faux négatifs) des filtres anti-hameçonnage;

[68] La statistique F produite par l'ANOVA est le rapport entre la variabilité inter et intra-groupes.

- quel est le degré de satisfaction ou d'insatisfaction à l'égard des développements des outils de formation (ex. en utilisant les micro-jeux).

En revanche, le degré de satisfaction à l'égard du temps moyen de mise à jour du fichier de journalisation au Canada semble plutôt influencé par le nombre d'années d'expérience en sécurité informatique. Les résultats exhaustifs de l'analyse de la variance de tous les énoncés de l'enquête sont présentés dans les tableaux L.1 à L.6 de l'ANNEXE L.

Tableau 7.7 : ANOVA à un facteur

Énoncé du questionnaire d'enquête	Facteurs qui influent sur le choix des experts	Somme des carrés	ddl	Carré moyen	F	Sig.
Meilleur réglage des critères de rejet	Niveau d'expérience en phishing	8,667	4	2,167	9,750	,009
Degré de satisfaction à l'égard des développements des outils de formation	Niveau d'expérience en phishing	5,722	2	2,861	5,421	,045
Degré de satisfaction à l'égard du temps moyen de mise à jour fichier de journalisation au Canada	Niveau d'expérience en sécurité informatique	6,889	3	2,296	5,741	,045

À la lumière du test de la variance que nous avons réalisé, l'hypothèse nulle est validée pour onze énoncés et rejetée pour les trois autres (cf. Tableau 7.7). Cela veut dire que les choix qui ont été faits pour les onze énoncés n'étaient, fort probablement, pas influencés par les différences dans les expériences des experts en sécurité informatique et en hameçonnage. Restent deux explications possibles: soit la mesure présente effectivement des insuffisances qui ne garantissent pas leur efficacité dans la lutte contre l'hameçonnage, soit que la question n'est pas suffisamment claire. Nous penchons plus pour la première raison car nous n'avons reçu aucun feedback relatif la non clarté de l'énoncé.

Pour les trois autres énoncés, les moyennes seraient différentes selon les groupes d'expérience. Toutefois, l'analyse ANOVA ne précise pas où sont situées ces différences et de combien sont-elles. Pour avoir ces informations, il faut faire des tests Post-hoc (a priori). Or, la taille restreinte de notre échantillon ne permet pas d'effectuer ces tests avec

les fonctions standards d'Excel car certains groupes possèdent moins de deux observations. Nous avons donc utilisé une macro VBA dans Excel pour déterminer la moyenne de chaque groupe. Les tableaux qui suivent présentent ces moyennes.

Tableau 7.8 : Moyenne de chaque groupe - expérience en hameçonnage-

Groupes	Meilleur réglage des critères de rejet	Degré de satisfaction à l'égard des développements des outils de formation	Degré de satisfaction à l'égard du temps moyen de mise à jour du fichier de journalisation au Canada
1 à 5 ans	2,8	3	2
6 à 10 ans	2,5	2	3
11 à 15 ans	3	3,5	3
16 à 20 ans	2	4	3

Tableau 7.9 : Moyenne de chaque groupe - expérience en sécurité informatique-

Groupes	Meilleur réglage des critères de rejet	Degré de satisfaction à l'égard des développements des outils de formation	Degré de satisfaction à l'égard du temps moyen de mise à jour fichier de journalisation au Canada
1 à 5 ans	3	3,33	?
6 à 10 ans	2,75	2,25	3
11 à 15 ans	3	3,25	2,67
16 à 20 ans	1,75	1,75	2,67

Les écarts entre ces moyennes ne suivent aucune logique qui nous permet de conclure à une influence de l'expérience sur le choix des experts.

Pour conclure, les choix qui ont été faits par les experts pour ces trois énoncés ne semblent pas avoir été influencés par les différences dans les expériences des experts en sécurité informatique et en hameçonnage. À l'instar de l'analyse que nous avons faite sur les onze autres énoncés, la seule explication qui semble plausible est que ces mesures ont des insuffisances qui ne garantissent pas leur efficacité dans la lutte contre l'hameçonnage, l'hypothèse selon laquelle les questions manqueraient de clarté étant peu plausible.

Pour la catégorie où le choix des réponses aux énoncés est très élevé ou élevé, nous additionnons les deux proportions de répondants pour obtenir une seule proportion que

nous qualifions de choix favorables des experts à l'énoncé. Ces mesures sont considérées dans la suite de notre travail comme des mesures recommandées pour la lutte contre l'hameçonnage bancaire.

7.2.2 Synthèse des résultats

Il ressort de cette enquête que six des neuf variables identifiées dans la revue de littérature comme étant des facteurs qui contribueraient à la monétisation récoltent plus de 50% des opinions favorables (élevé et très élevé) des experts (cf. Tableau 7.10 ci-dessous). Toutefois, nous avons noté des écarts importants entre ces résultats et ceux obtenus par simulation de notre modèle théorique et entre ces mêmes résultats et ceux d'un expert en criminologie qui est une référence dans le domaine. Le Tableau 7.10 ci-dessous présente les six facteurs retenus ainsi que les proportions des choix qui ont été faites par les experts pour chacun de ces facteurs. Nous reviendrons sur ces résultats au chapitre 8 afin de tenter de trouver une explication à ces écarts.

Tableau 7.10 : Facteurs de monétisation selon plus de 50% des experts

Rang	Facteurs	% d'experts ayant choisi le degré élevé	% d'experts ayant choisi le degré très élevé
1	Revenu anticipé par le fraudeur	38%	50%
2	Anonymat	31%	50%
3	Qualité du renseignement	31%	44%
4	Prix du renseignement	40%	33%
5	Temps écoulé depuis l'apparition du renseignement sur le marché	33%	33%
6	Niveaux des mesures mises en place par les banques	31%	19%
7	Probabilité	13%	13%
8	Richesse initiale	25%	0%
9	Commission versée à la mule	13%	0%

Relativement aux insuffisances des contremesures de sécurité relevées dans la revue de littérature, le tableau ci-dessous résume toutes les mesures pour lesquelles les répondants ont fait, à plus de 50%, les choix très élevé et élevé.

Tableau 7.11 : Contremesures à améliorer selon les avis des experts

Rang	Mesures	% d'experts ayant choisi le degré élevé et très élevé
1.	Authentification multifactorielle	83%
2.	Systèmes d'alerte anti-phishing actifs (intégrés) dans les navigateurs	82%
3.	Authentification de transaction en ligne par des protocoles 3D-Secure ou Verified By	69%
4.	Mécanismes d'empreinte avec authentification de l'émetteur	63%
5.	Signature numérique	59%
6.	Formation de base en sécurité	59%
7.	Campagne de sensibilisation continue aux enjeux de sécurité	59%
8.	Certificat EV SSL à validation étendue	53%
9.	Chiffrement des transactions	53%

Par ailleurs, ces mêmes experts indiquent que pour que ces mesures soient véritablement efficaces il faudrait des dispositions additionnelles. Par exemple, ils préconisent que pour que la signature numérique soit efficace, il faut bien implémenter la cryptographie. Il en est de même des mécanismes d'empreinte avec authentification de l'émetteur. Nous avons résumé ci-dessous les suggestions additionnelles des experts. Chaque mesure qui s'y trouve a été suggérée par au moins deux experts. Nous y reviendrons au chapitre huit pour analyser dans les détails ces suggestions.

1. L'élimination des options suivantes sur les navigateurs :
    a. remplissage automatique des formulaires;
    b. sauvegarde des mots de passe;
    c. persistance des sessions sur les navigateurs.
2. L'amélioration des méthodes de détection (ex. détection par bitsquatting)
3. Liste noire centralisée et un modèle commun pour en assurer le partage sous autorité légale (ex. liste noire des sites de phishing par province).
4. Un incitatif pour les usagers – renforcement positif-.
5. L'utilisation des questions de sécurité.
6. La géolocalisation de l'utilisateur via son IP;
7. La théorie du Nudge (Économie comportementale).

8. Formation/campagne (publicité gouvernementale à grande échelle) de façon continue.
9. Formation des jeunes (dès leur première utilisation d'un ordinateur).
10. Publier des vidéos sur la page personnelle des clients pour information.
11. Sensibiliser les clients lors des ouvertures de compte bancaire, clip sur sites bancaires.
12. Guide d'information pour les nouveaux arrivants dans les entreprises.
13. Ludification[69] (gamification en anglais - utilisation des jeux).

7.3 Discussion

Les résultats de cette enquête peuvent être analysés selon quatre perspectives, notamment : la perspective :

- de l'utilisateur final ;
- de l'entreprise ;
- du développeur de solution ;
- des organismes de lutte contre l'hameçonnage bancaire (ex. force policière).

7.3.1 Perspective de l'utilisateur final

Si l'on se place au niveau de l'utilisateur final, parmi les facteurs de monétisation retenus par la majorité des experts, ceux qui le concernent directement sont :

1) le temps écoulé depuis l'apparition du renseignement sur le marché;
2) le niveau des mesures mises en place par les banques.

Le temps écoulé depuis l'apparition du renseignement sur le marché fait référence à la durée entre le moment où le renseignement est volé et celui où il est monétisé. Cette durée influe sur la monétisation en ce sens que plus long il est, moins sont les chances de monétiser car la victime s'en aperçoit et prend des dispositions pour que la carte soit annulée. En ce sens le signalement à temps des incidents auprès des banques constitue une mesure de protection additionnelle qui réduirait le risque qu'il y ait monétisation selon les experts sondés. Malheureusement, ce n'est pas toujours le cas puisque nombre

[69] C'est l'utilisation des mécanismes de jeu dans le développement des sites web, des applications d'apprentissage, des réseaux sociaux avec pour objectif d'augmenter leur acceptabilité et leur utilisation.

d'utilisateurs ne réagissent pas toujours assez rapidement pour limiter les conséquences indésirables lorsqu'il y a vol de ses renseignements.

Quant au niveau des mesures mises en place par les banques, ce sont généralement des mesures opérationnelles pour lesquelles l'utilisateur final est censé être sensibilisé et participer activement à leur efficacité. Par exemple, l'authenticité des questions de sécurité dans les comptes, etc.

Parmi les améliorations des contremesures que suggèrent les experts dans cette enquête, quatre mesures peuvent être implémentées au niveau utilisateur, notamment :

- l'authentification multifactorielle ;
- systèmes d'alerte anti-hameçonnage actifs (intégrés) dans les navigateurs ;
- signature numérique ;
- formation de base en sécurité ;
- campagne de sensibilisation continue aux enjeux de sécurité.

L'authentification multifactorielle vient pallier le problème que posent de trop nombreux mots de passe. Le but : encourager les utilisateurs à prendre leur distance par rapport à ces mots de passe qui sont des sources de vulnérabilité. Il existe à cet effet des solutions que l'utilisateur peut prendre afin d'utiliser moins de mots de passe, en autant qu'il ait une formation de base en sécurité ou qu'il soit sensibilisé à l'existence desdites solutions. Généralement, l'authentification multifactorielle consiste en une combinaison de deux de ces trois éléments : une chose que l'utilisateur sait, une chose qu'il a et une chose qui le caractérise (ce qu'il est). L'amélioration que suggèrent les experts interrogés dans le cadre de cette enquête est d'ajouter une troisième clé qui peut être une paire de clés cryptographiques (clés publique et privée) afin de se débarrasser définitivement des mots de passe.

Toujours au niveau de l'utilisateur, 59% des experts sondés pensent que la signature numérique peut être une alternative efficace à la sécurisation des transactions en ligne. Toutefois, la formation et la sensibilisation de l'utilisateur et des banques sont des préalables à la mise sur pied d'une telle mesure. Aussi, signalons qu'une telle mesure exige

un tiers de confiance, encore appelé autorité de certification, qui fait office de vérificateur d'identité.

Enfin, une très grande majorité (82%) des experts favorisent les systèmes anti-hameçonnage intégrés dans les navigateurs pour pallier les limites des navigateurs présentées au chapitre 2. Nous pensons qu'une telle mesure, couplée à la suggestion que les experts ont faite d'éliminer les options de remplissage automatique des formulaires, de sauvegarde des mots de passe et de persistance des sessions sur les navigateurs, contribueraient davantage à réduire le risque de victimisation par tentative d'hameçonnage et de victimisation par infection.

7.3.2 Perspective de l'entreprise

L'entreprise ici englobe les fournisseurs Internet, les banques etc. La lecture des résultats de cette enquête selon la perspective de l'entreprise montre que parmi les facteurs de monétisation, le revenu anticipé, le temps écoulé depuis l'apparition du renseignement sur le marché et le niveau des mesures mises en place par les banques touchent directement les entreprises.

Rappelons que le revenu anticipé représente le montant disponible dans le compte personnel ou dans la carte de la victime. Et, comme nous l'avons mentionné au chapitre 6, plus ce montant est élevé, plus l'espoir de faire plus d'argent est grand et plus le fraudeur trouvera des voies et moyens pour monétiser le renseignement. Or, l'information sur ce montant est facilement accessible puisqu'elle fait partie des renseignements bancaires volés. Nous pensons qu'une des améliorations à apporter par les banques et les institutions qui gèrent les renseignements de cette nature serait de rendre plus difficile l'accès à cette information.

Pour les deux autres facteurs, notamment le temps écoulé depuis l'apparition du renseignement sur le marché et le niveau des mesures mises en place par les banques, les raisons des choix des experts sont les mêmes que celles évoquées pour la perspective de l'utilisateur.

En ce qui concerne les contremesures à améliorer, l'entreprise est touchée par toutes les mesures pour lesquelles les experts se sont prononcés à plus de 50% (cf. Tableau 7.11) et

ce, à des degrés divers. Par exemple, l'authentification multifactorielle est un concept qui s'intègre à la fois du côté client que sur des serveurs. C'est donc une solution nécessaire pour les entreprises et pour les utilisateurs. Il en est de même des autres mesures.

Parmi les suggestions des experts pour les mesures additionnelles, cinq d'entre elles touchent directement l'entreprise. Il s'agit de :

1 l'utilisation des questions de sécurité;

2 la géolocalisation de l'utilisateur via son IP;

3 la théorie du Nudge (Économie comportementale) ;

4 la sensibilisation des clients lors des ouvertures de compte bancaire ;

5 la production des guides d'information pour les nouveaux arrivants dans les entreprises.

7.3.3 Perspective du développeur de solutions

Le but d'analyser ces résultats d'enquête selon la perspective du développeur de solutions est de faire ressortir les mesures et suggestions qui peuvent contribuer à des développements efficaces des nouvelles contremesures. Dans cette optique, toutes les mesures d'amélioration pour lesquelles les experts se sont prononcés à plus de 50% (cf.Tableau 7.11) sont importantes pour le développeur en ce sens qu'elles sont toutes des applications logicielles. Aussi, il serait intéressant d'intégrer les suggestions suivantes dans les développements futurs :

1. l'amélioration des méthodes de détection (ex. détection des attaques bitsquatting) ;
2. l'intégration en amont des considérations humaines (ex. utilisation des questions de sécurité, interfaces de sécurité adaptées) ;
3. la géolocalisation de l'utilisateur via son IP ;
4. ludification (gamification en anglais - utilisation des jeux).

7.3.4 Revenu anticipé R

Pour analyser l'effet de la variation du revenu anticipé sur les quantités de renseignements q, nous postulons que :

- le montant maximum que le fraudeur peut soutirer par renseignement est égal à la limite l autorisée sur la carte de crédit ;
- les renseignements (ex. numéros de cartes de crédit) sont de même type (ex. pas de distinction carte platine, carte or, AMEX, VISA, etc.) et elles offrent les mêmes avantages, ont la même limite et le même solde. Cette hypothèse est introduite pour simplifier notre modèle. Sinon, on se retrouverait avec une multitude d'options pour chaque renseignement, ce qui complexifierait la tâche de modélisation. Toutefois, il n'est pas exclu que cette notion de qualité de renseignement fasse partir d'une étude ultérieure;
- le fraudeur qui veut augmenter son revenu anticipé R choisira parmi les renseignements achetés au marché noir, ceux pour lesquels il a plus de chance de soutirer les sous, c'est-à-dire les renseignements de meilleure qualité. Parmi les caractéristiques de la qualité, il y a le montant disponible dans le compte. Nous pensons donc que plus ce montant est élevé, plus l'espoir de faire plus d'argent est grand et plus il trouvera des voies et moyens pour monétiser plus de renseignements. L'hypothèse est donc que plus le revenu anticipé est élevé plus q augmente.

H6.2 : l'augmentation du revenu anticipé R a un impact positif sur la quantité q de renseignements monétisés

7.3.5 Perspective des organismes de lutte contre l'hameçonnage bancaire

Bien que nous n'ayons pas posé de questions spécifiques lors de notre enquête sur des améliorations éventuelles des solutions qui relèvent des organismes de lutte contre l'hameçonnage, certains experts ont suggéré quelques éléments de mesures qu'il vaut la peine de mentionner dans ce travail. Parmi ces mesures d'amélioration, certaines relèvent

aussi bien de l'entreprise que des organismes voire même des pouvoirs publics. À titre d'exemple, citons la sensibilisation aux menaces. En revanche, la collecte de données sur les menaces, la standardisation des normes, le renforcement des enquêtes policières et bien d'autres encore relèvent des organismes qui luttent contre l'hameçonnage. Nous nous limiterons dans cette présentation des résultats d'enquête à ces quelques éléments de mesures.

7.4 Conclusion

En initiant cette enquête, l'objectif était double. D'une part, nous voulions valider notre modèle théorique de monétisation avec les avis des experts et, d'autre part, confirmer les limites de certaines contremesures que nous avons identifiées par la revue de littérature et recueillir les avis d'amélioration que proposent les experts à ce sujet.

Le tableau qui se dégage de ces résultats est complexe, marqué par quelques rares avis largement partagés, des contradictions, suggestions d'améliorations très intéressantes et plusieurs zones grises. Ainsi, on retiendra que le degré d'accord entre les experts est très élevé (plus de 80%) sur le fait que les revenus anticipés du fraudeur et l'anonymat ont une plus grande influence sur le processus de monétisation, contrastant par exemple avec les avis mitigés de ces mêmes experts sur l'influence des contremesures mises en place par les banques pour réduire le risque de monétisation. Par rapport à ce facteur en particulier, plusieurs experts sondés pensent qu'une meilleure sensibilisation des clients (ex. lors de leur ouverture de compte) sur les enjeux mais aussi sur les contremesures que les banques mettent en place pour lutter contre le retrait non autorisé de l'argent des comptes des victimes réduirait le risque de cette forme de victimisation. C'est ce qui expliquerait que les avis sur cet énoncé soient aussi mitigés (50%).

Relativement aux contremesures étudiées, l'authentification multifactorielle et les systèmes d'alerte anti-hameçon intégrés dans les navigateurs sont largement partagés par plus de 80% des experts qui ont participé à cette enquête.

Pour les autres résultats, des disparités importantes ont été notées, d'une part entre les avis des experts et les résultats des travaux antérieurs et, d'autre part, entre les avis des experts de cette même enquête.

Les résultats qui ont été présentés dans ce chapitre nous permettent de compléter le troisième grand bloc de notre approche comme on peut le voir sur la figure 7.2 ci-dessous.

Le prochain chapitre apporte des nuances à ces résultats d'enquête et répond à la question principale de notre recherche.

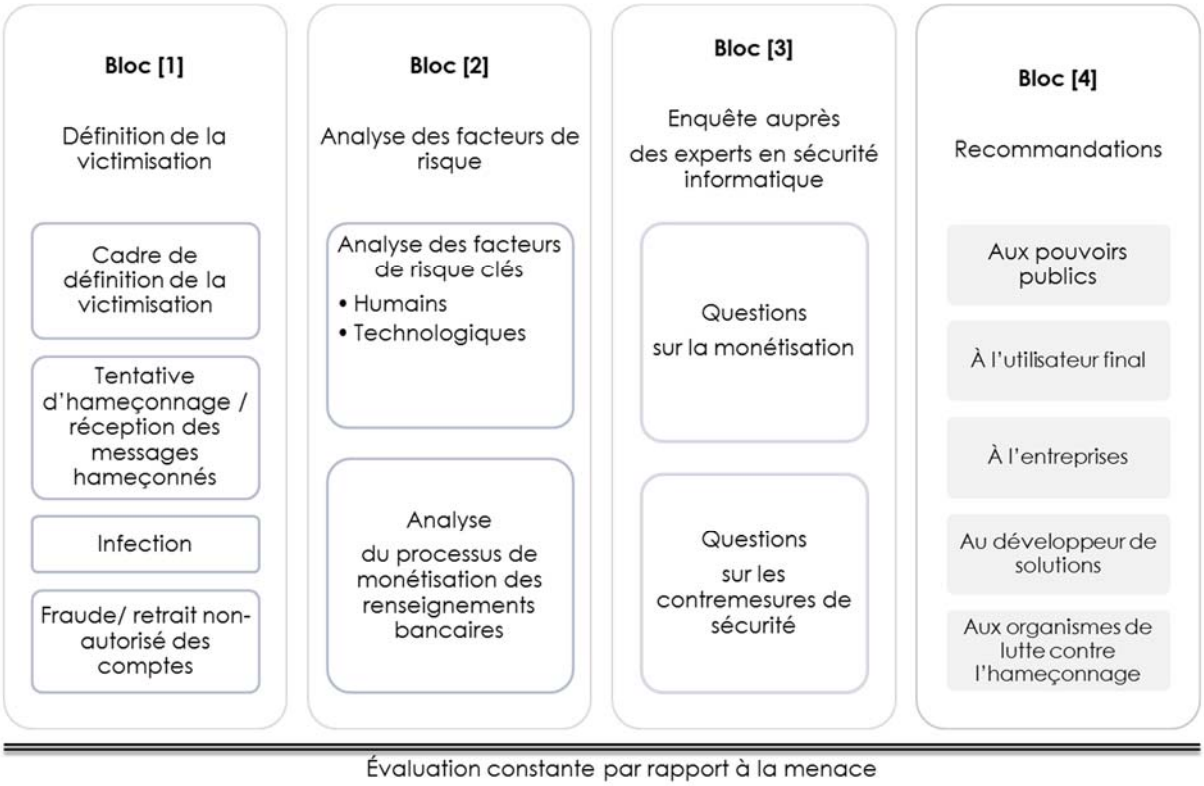


Figure 7.2 : Cadre d'analyse et de réduction de risque d'hameçonnage bancaire proposée

CHAPITRE 8 DISCUSSION ET RECOMMANDATIONS

Le précédent chapitre a permis de présenter les résultats de notre enquête menée auprès d'experts en sécurité informatique. Le présent chapitre, en se basant sur les analyses des avis de ces experts et sur notre propre expérience d'analyste en sécurité informatique, dresse un portrait des facteurs de risque d'hameçonnage bancaire et formule des recommandations destinées aux acteurs qui interviennent dans le processus de lutte contre l'hameçonnage bancaire. Ces recommandations constituent la principale contribution scientifique pratique de ce travail de recherche.

8.1 Facteurs clés de risque de victimisation par hameçonnage bancaire

Le point de départ de l'analyse des facteurs de risque a été une réflexion sur la victimisation. Nous avons voulu savoir ce qu'est la victimisation avant même de chercher à identifier les circonstances dans lesquelles elle se produit et les facteurs prédicteurs de victimisation. Le chapitre 4 a permis, à la fois de répondre à notre question Q1, et de définir le canevas qui a été utilisé au chapitre 5 pour répondre à la question de recherche Q2 relative aux facteurs clés de risque de victimisation par hameçonnage bancaire. Les résultats de la présente étude suggèrent globalement quatre types de facteurs clés de risque de victimisation :

- l'absence d'un cadre juridique contraignant;
- les facteurs humains;
- les limites et insuffisances des technologies;
- les facteurs propres au marché noir des renseignements bancaires.

L'absence d'un cadre juridique contraignant fait consensus aussi bien chez les experts consultés au cours de cette enquête (82%) que chez les auteurs des travaux antérieurs que nous avons examinés. Notons qu'il ne s'agit pas seulement d'une loi pour punir les auteurs de *phishing* ou pour dédommager les victimes de fraude par hameçonnage. Ce type de loi existe déjà dans plusieurs pays développés (McNealy, 2008; Pinguelo & Muller, 2011). Le cadre dont il est question ici est un ensemble de lois qui, non seulement facilitent les échanges entre les parties, entre les pays, mais aussi qui encadrent les actions de tous ceux et celles qui luttent contre la cybercriminalité dans son ensemble et, en particulier les forces de police.

Par rapport aux facteurs humains, un des résultats auquel nous sommes parvenus au chapitre 5 est que la fréquence d'utilisation d'internet pour les achats et opérations bancaires en ligne est le premier facteur de prédiction de la victimisation par tentative d'hameçonnage et de la victimisation par infection. Ces résultats valident en partie nos hypothèses H4.1.a et H4.2.a. Nous disons en partie parce qu'ils ne permettent pas de prédire le cas de victimisation par fraude. Ces résultats confirment en même temps l'hypothèse de Reyns (2015) selon laquelle la fréquentation des sites d'achat et des sites de banques constitue une plus grande exposition en ligne aux délinquants motivés (Reyns, 2015). Toutefois, il est important de mentionner ici que ce n'est pas une relation déterministe. Le fait d'utiliser internet pour ce type de transactions génère des opportunités cybercriminelles et en soi offre des tentations, des motivations aux attaquants (Cohen & Felson, 1979) mais ne constitue pas la cause profonde de tentative ou d'infection par hameçonnage. Nous reviendrons plus loin sur cette notion de causes sous-jacentes.

Autre résultat que nous avons obtenu : les personnes qui utilisent les salons de clavardage et les réseaux sociaux sont plus susceptibles de se faire infecter que celles qui ne les utilisent pas. Cette conclusion n'est pas nouvelle car plusieurs auteurs ont établi ce lien entre l'utilisation des réseaux sociaux et le taux d'infection. C'est le cas de Liu et al. (Liu, Hsu, & Ke, 2014). Notre étude confirme ce lien avec un plus grand échantillon de répondants et, par conséquent, de données plus fiables. Notre hypothèse H4.2.b est donc validée alors que les hypothèses H4.1.b et H4.2.b ne sont pas.

Nous avons constaté aussi que certaines caractéristiques sociodémographiques et économiques, comme le fait de vivre en région, d'être un homme, d'être scolarisé, de parler anglais ou d'être riche avaient pour effet d'augmenter le risque d'être victime de tentative d'hameçonnage et d'infection. Au chapitre 5, nous avons donné une explication aux corrélations que nos analyses ont permis d'établir entre ces facteurs et chacune des formes de victimisation que nous avons étudiées dans ce travail. Des études antérieures se sont penchées sur ces facteurs et nos résultats corroborent plusieurs d'entre elles. Par exemple, notre conclusion à l'effet qu'être scolarisé augmente le risque d'être victime de tentative d'hameçonnage et d'infection confirme les résultats de Graham et al. (2016) qui indiquent que l'alphabétisation numérique influe de manière significative sur la réception des courriels hameçonnés et sur les infections par hameçonnage (Graham & Triplett, 2016). Cependant, nos résultats ont principalement porté sur l'identification de prédicteurs clés plutôt que sur l'origine de corrélations que nous avons trouvées ou encore sur leur causalité. Nous

croyons qu'une meilleure compréhension des différences sociodémographiques passe par une future recherche sur les liens potentiels entre l'aversion au risque des utilisateurs et la victimisation par hameçonnage bancaire. Nous pensons qu'une telle étude pourrait expliquer, par exemple, pourquoi le fait d'être un homme a pour effet d'augmenter le risque d'être victime de tentative d'hameçonnage et d'infection. Il est donc suggéré d'étudier les causes sous-jacentes de ces différences sociodémographiques.

L'autre piste de réflexion à investiguer pour les travaux futurs concerne le risque moral et la victimisation par hameçonnage bancaire. Cette recherche exploratoire nous a conduit à nous demander si le fait de prendre des contremesures peut être un incitatif à la prise de risque. Les résultats de l'analyse préliminaire que nous avons réalisée au chapitre 5 sur cette question indiquent qu'il semble y avoir un lien probable entre le fait de prendre des contremesures et l'adoption, par l'internaute, de comportements susceptibles d'augmenter le risque de victimisation par tentative d'hameçonnage et par infection. Toutefois, les écarts entre les mesures d'associations des variables que nous avons utilisées pour cette analyse ne sont pas suffisamment élevés. Pour cette raison, nous ne pouvons tirer de conclusion définitive.

Enfin, sous cette même rubrique relative aux aspects humains, deux facteurs de risque de victimisation sont revenus le plus souvent dans cette étude : le manque de formation de base et de sensibilisation aux enjeux de sécurité. Ces deux facteurs relèvent aussi bien de l'utilisateur que des entreprises voire des pouvoirs publics. Ils ont des incidences majeures à tous les niveaux du processus d'hameçonnage bancaire, que ce soit pour reconnaître un URL qui contient un nom de domaine trompeur ou pour utiliser des mots de passe forts ou encore pour détecter une défaillance d'un antivirus par exemple, l'utilisateur a besoin d'un minimum d'informations et de connaissances sur les menaces et les contremesures. Le degré d'insatisfaction moyenne des experts que nous avons sondés à l'égard de ces deux facteurs et que nous avons présenté au chapitre 7 varie entre 40% et 76%. Ces chiffres n'incluent pas les avis des experts qui n'étaient ni en accord, ni en désaccord. Aussi, ils confirment les résultats de la revue de littérature faite au chapitre deux et relatifs aux limites des programmes formation et de sensibilisation.

Les raisons évoquées par les experts sondés pour justifier leur insatisfaction sur les formations et campagnes de sensibilisation sont les suivantes :

- les formations ne sont pas renouvelées chez les utilisateurs alors que les menaces, elles, changent à un rythme effréné;
- les interfaces de communication qui viennent en support à la formation ne sont pas mises à jour régulièrement;
- les programmes de formation en place ne sont pas toujours adaptés à l'auditoire et à la gravité des menaces;
- lors des formations, les tests sont effectués avec des scénarios prédéfinis où les sites d'hameçonnage sont connus d'avance (Purkait, 2012).

Afin de répondre à notre question de recherche Q6, nous avons interprété ce haut degré d'insatisfaction comme une mesure de l'importance que ces experts accordent aux formations et campagnes de sensibilisation telles qu'elles sont offertes en ce moment. Et, en ce sens, cette importance est plutôt très faible.

En ce qui concerne les facteurs de risque de victimisation liés aux technologies, le point de départ de l'analyse qui suit a été l'examen de la littérature que nous avons fait au chapitre 2. Nous y avons identifié un certain nombre de limites et défaillances des contremesures et, notamment, celles d'ordre technologique. Par exemples, les filtres anti-hameçonnage souffrent d'un taux élevés d'erreurs alors que la signature numérique nécessite des coûts d'implémentation et de formation très élevés. Une analyse exhaustive de ces facteurs a permis de répertorier les facteurs suivants :

1. le taux élevé d'erreurs des filtres anti-hameçonnage en raison de mauvais réglage;
2. la défaillance ou l'absence des contremesures de base comme l'anti-virus, le pare-feu, les mises à jour de sécurité, etc.;
3. les coûts élevés de la signature numérique;
4. la gestion de multiples mots de passe, les vulnérabilités des navigateurs et des barres d'outils;
5. les coûts élevés des systèmes experts;
6. les limites du chiffrement des transactions en raison de la mauvaise implémentation de la cryptographie.

En y regardant de plus près, plusieurs de ces limites renvoient au jugement et au comportement de l'utilisateur face aux contremesures et à la menace. Par exemple, le réglage des critères de rejet des filtres anti-hameçonnage peut s'avérer une épée à double tranchant car si on ne resserre pas assez les règles, on risque de se retrouver avec de faux négatifs (courriels hameçonnés non détectés). En

revanche, si on les resserre un peu trop, cela peut engendrer des faux positifs (ex. on peut mettre un contrat important dans les courriels indésirables et faire perdre des sommes importantes à une entreprise). Alors, jusqu'où on peut aller dans le resserrement des règles ? C'est juste une question de jugement que tout utilisateur doit avoir et, pour ce faire, il a besoin d'être bien formé sur ces technologies et sur les menaces.

En appliquant le même raisonnement au second facteur de risque de victimisation ci-dessus, on se rend compte qu'il est très difficile d'établir clairement quelle est la cause profonde de la défaillance d'un antivirus, par exemple. Est-ce qu'une telle défaillance relève d'une cause purement technologique ou d'un manque de connaissances de base en sécurité ? La même question peut se posée pour la gestion des mots de passe ou pour la vulnérabilité des navigateurs.

Il ressort de cette analyse que ce n'est pas seulement la dimension technologique qui est en cause mais une combinaison de celle-ci et du manque de formation ou de familiarisation avec les filtres. Ce constat soulève un autre problème : celui de l'intégration des considérations humaines tôt dans le développement de ces solutions technologiques.

En résumé, nous avons retenus les six facteurs identifiés plus haut comme facteurs clés de victimisation, non pas parce que les technologies sont déficientes à proprement parler, mais parce que leur utilisabilité induit des risques de victimisation. Le tableau 8.3 ci-dessous décrits les recommandations tirées des avis des experts pour pallier ces facteurs et répondre à nos questions Q3 et Q4 relatives aux améliorations à apporter aux filtres ainsi qu'à la sécurisation des navigateurs.

Relativement au marché noir des renseignements, le modèle théorique que nous avons développé a permis de classifier les facteurs qui contribuent à la monétisation des renseignements en utilisant des données de simulation tirées d'Internet. Afin de valider les résultats de simulation de ce modèle théorique, nous avons demandé à dix-sept experts en sécurité informatique de classer, sur une échelle de 1 à 5, l'influence de chacun de ces facteurs sur les chances de monétiser les renseignements bancaires volés par hameçonnage. La Figure 8.1 suivante compare les résultats du classement des facteurs de monétisation issus de la simulation du modèle théorique avec la moyenne des avis d'experts ainsi qu'avec l'opinion d'un d'entre eux en particulier en raison de sa longue expérience et son expertise bien assise dans l'analyse des forums clandestins.

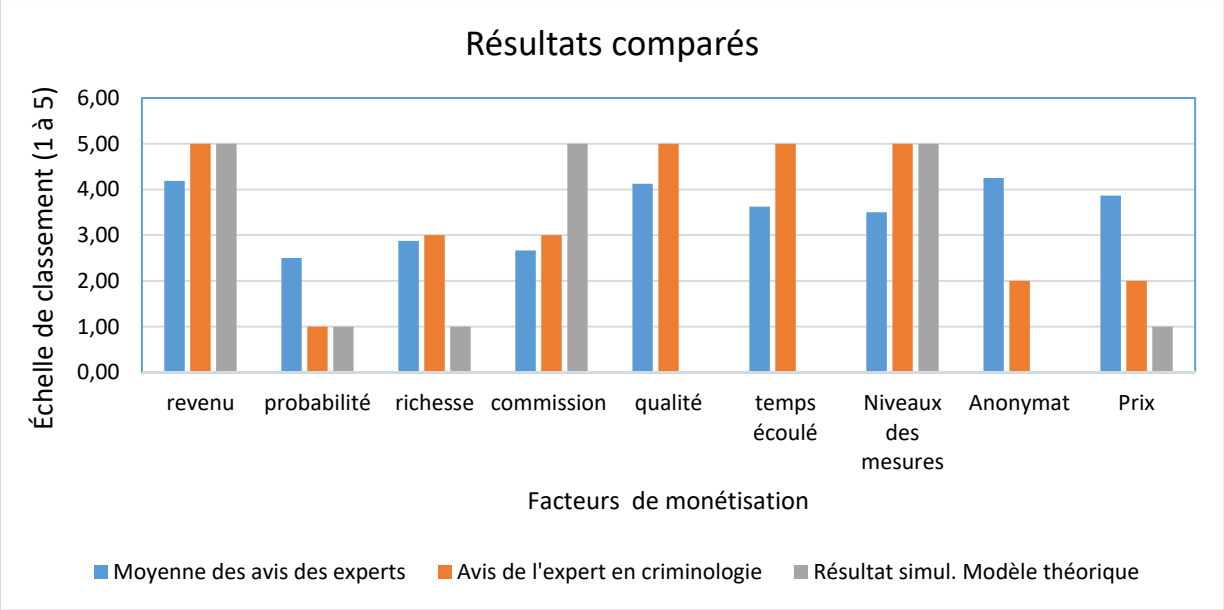


Figure 8.1 : facteurs qui influent sur le processus de monétisation

Sans surprise, on y découvre que, pour 82% des experts, le premier facteur de monétisation est l'appât du gain du fraudeur, c'est-à-dire le montant qu'il espère retirer du compte de sa victime. La moyenne des avis d'experts relatifs à ce facteur est de 4,2 sur 5 alors que le résultat de simulation du modèle théorique est équivalent au choix de 5, à égalité avec le score de l'expert en criminologie.

Ce résultat est conforme à ce qui ressort de la revue de la littérature sur la fraude en générale. Aussi, il confirme les résultats du sondage 2013 mené par la firme KPMG pour le compte de la banque mondiale. KPMG a suivi les fraudeurs et analysé leur comportement entre 2011 et 2013. Sur 1082 réponses précises, 614 (57%) ont indiqué que les motifs de fraude étaient la cupidité, le gain financier ou des difficultés financières (KPMG, 2013).

Quant au deuxième facteur, les avis sont partagés entre l'influence qu'exerce le niveau des mesures mises en place par les banques et la qualité du renseignement, avec un léger avantage pour le premier qui récolte une moyenne des avis d'experts de 3,5 sur 5 et un résultat équivalent à 5 avec le modèle théorique, à égalité également avec le score de l'expert en criminologie. Notons que le niveau des mesures de sécurité prises par les banques réduit le risque de monétisation alors que la qualité du renseignement peut exercer une influence favorable à la fraude. Ce sont donc deux facteurs aux effets opposés.

Signalons également que notre modèle théorique n'a pas mesuré la qualité du renseignement en raison de la complexité que présenterait la modélisation de ce paramètre. Il en est de même du temps écoulé entre le vol du renseignement et la fraude et de l'anonymat. Pour ces trois facteurs, nous ne considèrerons dans cette analyse que la moyenne des avis des experts en sécurité et l'opinion du spécialiste en criminologie.

En suivant cette même logique d'analyse, c'est-à-dire en comparant les résultats des trois évaluations, le temps écoulé arrive en quatrième rang, suivi de la commission versée à la mule, de la richesse initiale du fraudeur, puis de l'anonymat et du prix du renseignement. Quant à la probabilité de se faire arrêter, elle occupe la dernière place dans la liste. La partie droite de la Figure 8.2 ci-dessous résume ce classement des facteurs de monétisation.

Par ailleurs, cette étude a révélé que la commission versée à la mule n'a pas l'importance que lui accordent certaines publications antérieures comme celle de Panda Security (Panda, 2011). Ceci s'explique par le fait qu'avant même que la mule n'intervienne dans le processus de conversion d'un renseignement, il y a des préalables. Par exemple, il y a la durée du renseignement sur le marché qui doit être très courte faute de quoi la mule ne peut exploiter le renseignement. De plus, il faut passer à travers les questions de sécurité des banques. Voilà autant de raisons qui expliquent que le rôle de la mule et la commission qui lui est versée ne soient pas des facteurs déterminants.

Cette étude a confirmé que le prix du renseignement et la richesse initiale du fraudeur n'ont que peu d'importance, les renseignements se transigeant dans les forums clandestins à des prix de l'ordre de quelques cents.

L'anonymat est considéré dans cette étude comme un facteur résiduel car il n'est pas propre à la fraude et son influence n'est pas spécifique à la monétisation.

En résumé, nous avons retenu les quatre facteurs clés ci-dessous (cf. Tableau 8.1) parce que leur influence sur le processus de monétisation recueille des avis favorables d'une large majorité d'experts consultés et parce que l'analyse et la simulation de notre modèle théorique confirment cette influence pour deux d'entre eux, les deux autres n'ayant pas été mesurés.

Tableau 8.1 : Facteurs clés du processus de monétisation

Facteurs	**Impact du facteur**
1. Revenu anticipé par le fraudeur	Plus il est élevé, plus grande est la motivation du fraudeur pour monétiser
2. Niveau de mesures mises en place par les banques	Plus il est élevé, moins sont les chances de monétiser
3. Qualité du renseignement	Plus elle est bonne, plus grands sont les chances de monétiser
4. Temps écoulé entre le vol du renseignement et la fraude	Plus court est ce temps, plus grands sont les chances de monétiser

La Figure 8.2 qui suit résume les éléments clés de l'analyse que nous venons de réaliser et répond de façon explicite à la question Q2 de notre recherche, à savoir :

Q2. : Quels sont les facteurs clés de risque de victimisation par hameçonnage bancaire ?

Ils sont d'ordre juridique, humain, technologique et inhérent au marché noir comme le détaille chaque catégorie de cette figure.

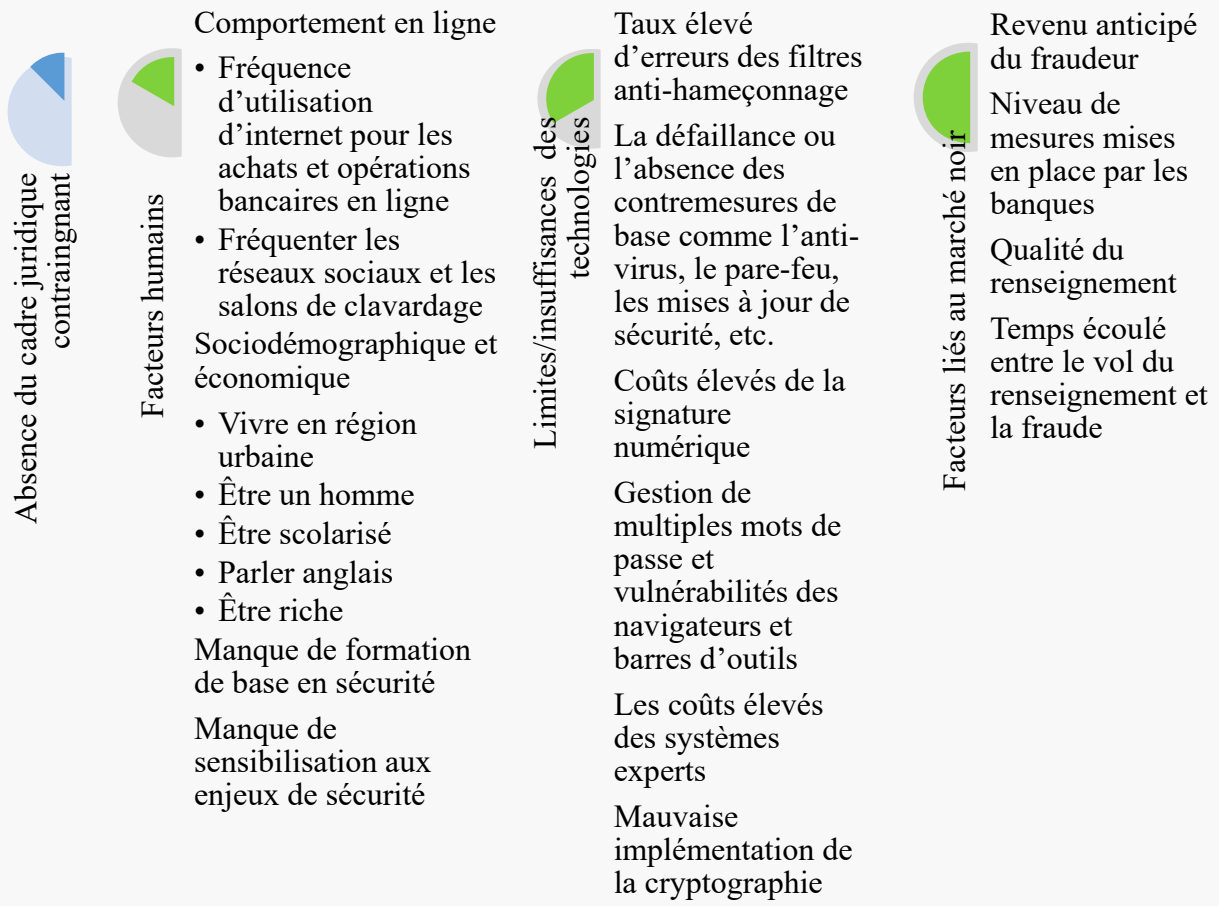


Figure 8.2 : Facteurs clés de risque de victimisation par hameçonnage bancaire

8.2 Recommandations

Nous avons fait le choix d'étudier séparément les recommandations qui sont destinées aux pouvoirs publics des solutions de type contremesure. Dans cette perspective, la première rubrique qui suit présente un certain nombre d'éléments que nous avons regroupés sous l'appellation recommandations aux pouvoirs publics.

8.2.1 Recommandations aux pouvoirs publics

Les experts sondés sont favorables à près de 84% à la mise en place d'un cadre juridique contraignant qui oblige les acteurs à échanger les informations nécessaires à la mise à jour des listes noires à l'intérieur d'un même pays et avec d'autres pays. La question qu'il faut se poser est de savoir si c'est possible et, dans l'affirmative, comment peut-on le faire ? Pour répondre à cette question, si l'on se réfère aux suggestions de ces mêmes experts, il faudrait désigner une autorité

en charge de coordonner les actions des différents acteurs et lui conférer les pouvoirs nécessaires pour mener à bien son mandat. C'est là une des difficultés majeures comme le fait remarquer Smyth dans son article (S. M. Smyth, 2014). De toute évidence, il n'y a pas d'autorité centrale ou de police pour Internet. Qui plus est, les décideurs au sein des organismes publics nationaux n'ont pas autorité sur toutes les alternatives, décisions et instruments de contrôle nécessaires pour apporter des changements considérables à ce genre de problème (Levin, Cashore, Bernstein, & Auld, 2012). La difficulté à coordonner les politiques entre de nombreux intervenants issus de multiples secteurs (éducation, santé, économiques, politiques, etc.) rend également difficile la réalisation d'une action collective (Levin et al., 2012). Pour toutes ces raisons et au regard des structures de lutte actuelle qui fonctionnent, pour la plupart, en silo, un tel cadre juridique semble être une avenue très difficile. En revanche, nous avons exploité quelques-unes des idées suggérées par les experts pour faire les recommandations suivantes :

Tableau 8.2 : Recommandations aux pouvoirs publics

Recommandations	**Responsabilité**
1. Créer des incitatifs fiscaux afin de favoriser la collaboration des acteurs des secteurs public et privé dans la lutte contre l'hameçonnage bancaire	Fédéral/provinciale
2. Intégrer dans les programmes scolaires des ateliers obligatoires de formation en sécurité informatique et y associer des incitatifs (ex. notes) - renforcement positif -	Provinciale
3. Donner plus de ressources aux forces policières et organismes de sensibilisation qui luttent contre l'hameçonnage bancaire.	Fédérale/Provinciale/municipale

À la lumière de l'analyse que nous venons de faire, la réponse à notre question Q5 est mitigée : un cadre juridique contraignant serait très difficile à mettre sur pied, l'hameçonnage bancaire spécifiquement n'étant pas considéré comme un enjeu de sécurité nationale. En revanche, une mesure incitative comme celle que nous recommandons par exemple en 1) pourrait favoriser l'émergence de nouvelles plateformes de partage d'informations sur l'hameçonnage bancaires à l'instar de ce qui se fait dans le domaine du crédit où des entreprises privées comme EQUIFAX et Trans Union qui se sont démarquées en prenant le leadership dans la gestion instantanée des données de crédit. L'idée ici est qu'une entité (organisme étatique ou sous-traitant privé) développe

et gère en temps réel une liste noire nationale des sites d'hameçonnage selon un modèle d'affaire qui offre à des clients un incitatif avec une attention toute particulière pour les hébergeurs de sites Web. Avec de telles mesures, combinées aux lois qui existent déjà (ex. Loi canadienne anti-pourriel –LCAP-, etc.) nous pensons qu'une grande partie des sites d'hameçonnage seraient mis hors d'état de nuire dans des délais assez courts en autant que les listes noires soient distribuées plus rapidement. De la sorte, la réduction du risque de victimisation serait possible à moyen terme.

8.2.2 Recommandations à l'utilisateur final

Globalement, les résultats de cette recherche confirment un constat qui a été fait au chapitre deux suite à l'examen de la littérature et qui est partagé par une large majorité des experts sondés lors de notre enquête : «les utilisateurs sont toujours les principaux maillons faibles de la cyber-sécurité» (Proofpoint, 2017). Il était donc très important, dans ce travail, de bien identifier les facteurs de risque de victimisation qui relèvent de l'utilisateur final afin de s'assurer de la justesse de nos recommandations, lesquelles recommandations sont regroupées ci-dessous en deux catégories de contremesures : les contremesures techniques et les contremesures éducatives et de sensibilisation.

a) Contremesures techniques

Lors de notre enquête, nous n'avons pas posé de questions sur l'efficacité des contremesures techniques de base (ex. antivirus, pare-feu et mises à jour de sécurité) car la revue de littérature ne l'identifie pas comme étant une source prioritaire de risque d'hameçonnage. En revanche, le manque d'éducation sur ces mêmes contremesures et notamment sur les alertes que génère par exemple l'antivirus constitue un facteur de risque clé. Par ailleurs, ces contremesures techniques de base ne visent pas spécifiquement l'hameçonnage bancaire. Pour ces raisons, nous les considérons comme un minimum de mesures requises. Nous préférons formuler des recommandations pour les facteurs de risque spécifiques à l'hameçonnage bancaire que nous avons déterminés plus haut. Ainsi, nous formulons sept recommandations relatives aux contremesures techniques pour aider l'utilisateur final à réduire le risque de victimisation.

Tableau 8.3 : Recommandations techniques à l'utilisateur final

Recommandations	**Réduit le risque lié**
1. Utiliser le mécanisme d'empreinte avec authentification de l'émetteur + bonne implémentation de la cryptographie	Au taux d'erreurs des filtres anti-hameçon
2. Utiliser la signature numérique + bonne implémentation de la cryptographie	Au taux d'erreurs des filtres anti-hameçon
3. Utiliser l'authentification multifactorielle	À la gestion des mots de passe des navigateurs
4. Activer/configurer le système d'alerte anti-hameçonnage	À la vulnérabilité des navigateurs
5. Activer le certificat EV SSL à validation étendue	À la vulnérabilité des navigateurs
6. Éliminer les options suivantes : a. Remplissage automatique des formulaires b. Sauvegarde des mots de passe c. Persistance des sessions dans les navigateurs	À la gestion des mots de passe et à la vulnérabilité des navigateurs
Mettre à jour régulièrement les RIA (Rich Internet Application)	À la vulnérabilité des navigateurs

Des sept recommandations que nous venons de faire, les deux premières répondent favorablement à notre question de recherche Q3 : l'utilisation des mécanismes d'empreintes avec authentification et de la signature numérique couplée à la cryptographie contribueraient à réduire les taux d'erreurs des filtres anti-hameçonnage. Quant à la question Q4, la réponse est donnée par les cinq autres recommandations. Et, comme nous l'avons mentionné au paragraphe 8.1, ces améliorations techniques devraient être combinées aux mesures éducatives et de sensibilisation pour plus d'efficacité.

b) Contremesures éducatives et de sensibilisation

Le résumé des facteurs clés de risque de la Figure 8. ci-dessus confirme clairement que les éléments prédicteurs de risque sont bien plus liés aux caractéristiques sociodémographiques de l'utilisateur ainsi qu'à son comportement devant la menace qu'aux technologies à proprement parler. Nos

recommandations sur les contremesures à prendre à cet effet visent essentiellement à pallier les problèmes engendrés par les comportements à risque et non ceux liés aux facteurs sociodémographiques, les causes sous-jacentes de ces derniers facteurs n'étant pas connues.

Tableau 8.4 : Recommandations éducatives à l'utilisateur final

Recommandations	**Réduit le risque lié**
1. Assister régulièrement aux campagnes de sensibilisation aux enjeux de sécurité	Aux menaces en général
2. Suivre une formation de base en sécurité / être sensibilisé aux menaces	Aux menaces et aux contremesures
3. Signaler à temps tout incident	À la monétisation
4. Prendre de mesures sécuritaires pour : a. gérer les mots de passe que l'on utilise; b. définir les questions de sécurité en combinaison avec d'autres critères d'identification; c. diversifier les outils et plateforme de navigation (ex. utiliser certaines plateformes sécurisées exclusivement pour les transactions impliquant les renseignements bancaires).	Aux menaces et aux contremesures

8.2.3 Recommandations à l'entreprise

En plus de toutes les recommandations que nous venons de faire à l'utilisateur final, nous recommandons à l'entreprise les améliorations suivantes :

Tableau 8.5 : Contremesures techniques

Recommandations	**Réduit le risque lié**
1. Améliorer l'authentification de transaction en ligne (3D-Secure, Verified By)	Aux transactions en ligne
2. Améliorer le chiffrement des transactions	Aux transactions en ligne
3. Utiliser davantage la géolocalisation	Aux transactions en ligne

Tableau 8.6 : Contremesures éducatives et de sensibilisation

Recommandations	**Réduit le risque lié**
1. Sensibiliser les clients lors des ouvertures de compte bancaire par des clips sur sites bancaires	Aux transactions en ligne
2. Produire des guides d'information pour les nouveaux arrivants dans les entreprises	Aux transactions en ligne
3. Utiliser obligatoirement les questions de sécurité	Aux transactions en ligne
4. Offrir des campagnes de sensibilisation continues.	Aux transactions en ligne

8.2.4 Recommandations aux organismes de lutte contre l'hameçonnage

Les recommandations que nous faisons dans cette rubrique sont tirées des suggestions de nos experts de la revue de littérature consultée.

Tableau 8.7 : Contremesures administratives

Recommandations	**Responsabilité**
1. Faire plus d'enquêtes, notamment auprès des banques, dans les forums clandestins et des experts	Organisme /Université
2. Produire plus de données empiriques sur les menaces à travers le monde et les contremesures	Organisme /Université
3. Mener plus de campagnes de sensibilisation auprès des décideurs	Organisme /entreprise
4. Utiliser les réseaux sociaux/nouveaux médias pour mener les campagnes de sensibilisation	Organisme /entreprise

De toutes les recommandations que nous avons faites, il y a une qui est revenue plus souvent que les autres : l'éducation de base en sécurité et la sensibilisation aux menaces. Les experts sondés sur

leur degré de satisfaction ont fait des suggestions très intéressantes sur des améliorations à apporter aux formations et campagnes de sensibilisation actuelles. Nous les avons déjà répertoriées au chapitre 7. On y trouve un peu de tout : de la publicité gouvernementale aux formations obligatoires en entreprise en passant par des capsules vidéos sur des pages Facebook.

En regardant de près ces suggestions d'experts, la réponse à notre question Q7 de recherche sur les améliorations à apporter aux formations et campagnes de sensibilisation est mitigée. D'abord, parce qu'il serait illusoire de penser que ces améliorations forceraient, par exemple, un utilisateur à y trouver un intérêt et ensuite parce que c'est une question d'argent. Quel employeur serait prêt à payer une formation de base en sécurité à tout nouvel employé ? Et, quel citoyen serait prêt à défrayer les coûts d'une telle formation de ses poches ?

8.3 Conclusion

Les facteurs clés de risque de victimisation par hameçonnage bancaire se résument en quatre catégories (cf. figure 8.2) :

- une absence d'un cadre juridique contraignant ;
- l'adoption par les utilisateurs de certains comportements à risque en ligne ;
- certaines caractéristiques sociodémographiques et économiques ;
- les limites des filtres anti-hameçon et des navigateurs ;
- les facteurs liés au marché noir des renseignements bancaires.

La figure 8.3 qui suit résume l'ensemble des améliorations à apporter aux contremesures de sécurité.

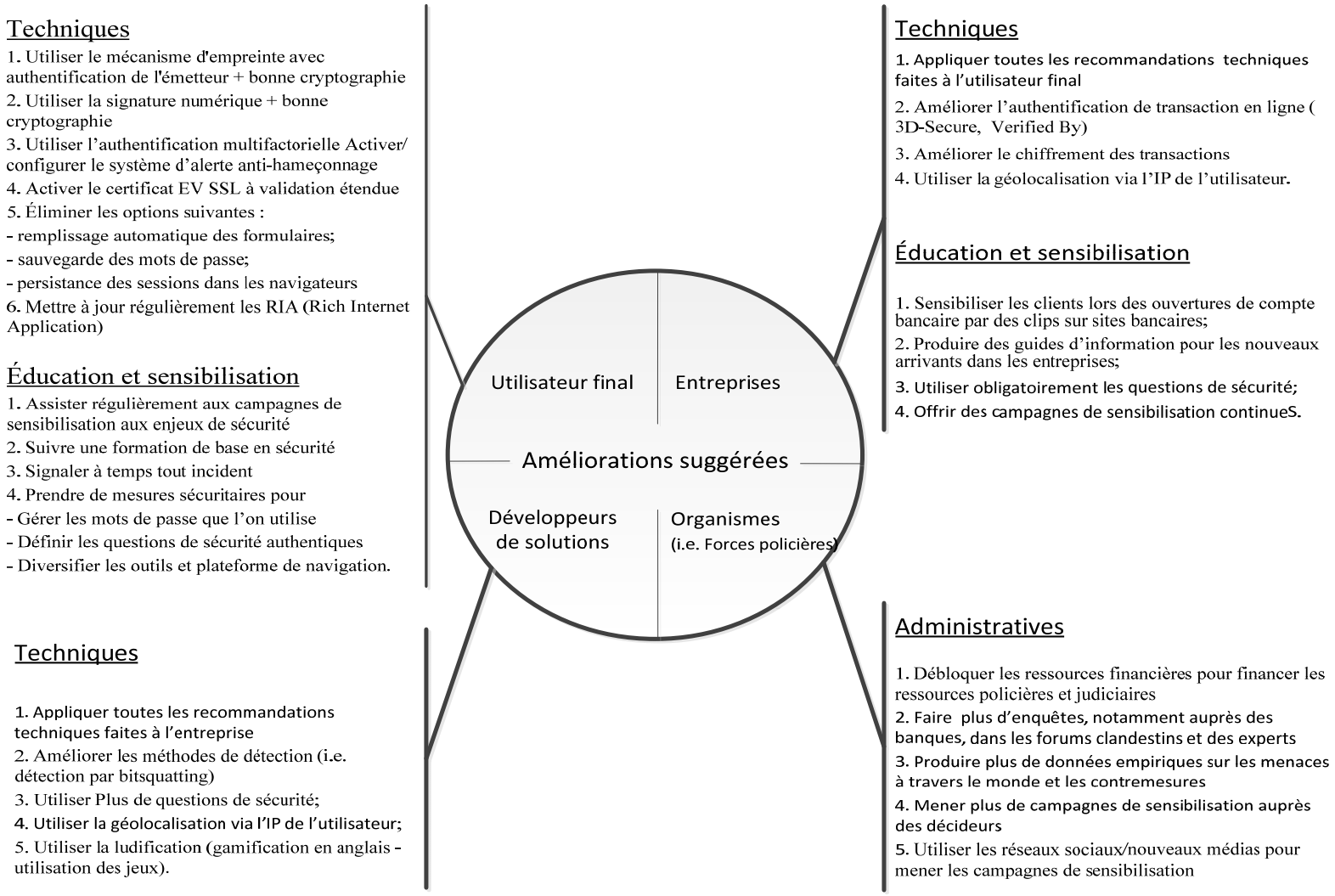


Figure 8.3 : Recommandations sur les améliorations des contremesures

CHAPITRE 9 CONCLUSION

Ce chapitre apporte des réponses précises à notre question principale de recherche. Pour ce faire, nous avons traité plusieurs sous-questions dans ce travail. Nous les résumons dans la section une qui suit. La section deux passe en revue les résultats présentés dans les chapitres quatre, cinq, six, sept et huit. Les limites de cette recherche sont présentées à la section trois, suivie, à la section quatre des contributions de cette thèse à la recherche. Nous concluons avec les enjeux futurs.

9.1 Rappel de la question de recherche

L'objectif de cette recherche était de répondre à la question générale qui est de savoir si un cadre d'aide à la lutte contre l'hameçonnage bancaire auquel différents acteurs vont recourir pour réduire le risque de victimisation est possible.

Pour répondre à cette question générale, plusieurs sous-questions ont été traitées, notamment :

Q1. Quels sont les éléments nécessaires et suffisants à la définition de la victimisation par hameçonnage bancaire ?

Q2. Quels sont les facteurs clés de risque de victimisation par hameçonnage bancaire ?

Q3. Quelles améliorations peut-on apporter aux filtres anti-hameçonnage afin de réduire les taux d'erreurs (ex. faux positifs ou faux négatifs) ?

Q4. Comment rendre les navigateurs plus sécuritaires à l'encontre des pirates ?

Q5. Un cadre juridique contraignant visant à favoriser l'échange des listes noires entre partenaires à l'intérieur d'un même pays et avec d'autres pays réduirait-il le temps de mise à jour de ces listes ?

Q6. Quelle est l'importance accordée aux formations en sécurité et aux campagnes de sensibilisation sur les menaces dans les organisations ?

Q7. Comment peut-on améliorer les formations et les campagnes de sensibilisation aux enjeux de sécurité?

Une approche d'analyse de risque de victimisation par hameçonnage bancaire a été développée en s'appuyant sur :

- la revue de littérature;
- un cadre de définition de la victimisation;

- un modèle d'analyse des facteurs de risque;
- un modèle théorique d'analyse du marché noir.

Puis, une enquête de terrain réalisée auprès de dix-sept experts en sécurité information a permis de valider les résultats de notre modèle théorique de monétisation et de suggérer, sous forme de recommandations, des améliorations à apporter aux mesures de lutte contre l'hameçonnage bancaire.

9.2 Le cadre d'analyse et de réduction du risque d'hameçonnage proposé

Nous avons prouvé qu'un tel cadre est possible et celui que nous proposons suggère de :

1. définir le type de victimisation pour lequel on veut analyser et réduire le risque de survenance;
2. décrire l'ensemble des activités qui conduisent à ce type de victimisation et, pour chaque étape, identifier les facteurs clés par une analyse croisée des facteurs issus de l'examen de la littérature et des réponses des victimes obtenues par une enquête;
    a. En l'absence de données empiriques sur certaines étapes, modéliser la chaine d'activités inhérentes à ces étapes et valider /tester le modèle théorique avec des données colligées soit du domaine publique, soit d'une enquête.
3. pour chaque facteur clé, colliger et analyser les avis d'experts sur les mesures à prendre pour atténuer le risque de victimisation;
4. Faire des recommandations aux parties prenantes.

Voilà, globalement en quatre étapes l'approche que nous préconisons dans cette thèse pour analyser et réduire le risque d'hameçonnage bancaire. La figure 9.1 ci-dessous schématise l'ensemble de ces étapes où chaque bloc représente un chapitre de cette thèse.

Comme préalable à la première étape, nous avons réalisé, au chapitre 2, une revue de littérature qui transcende les frontières de la sécurité informatique pour examiner ce qui s'est fait en économie du crime. Puis, nous avons proposé au chapitre 4 (première étape), en réponse à notre question de recherche Q1, un cadre de définition de la victimisation par hameçonnage bancaire qui s'articule autour de quatre groupes d'éléments clés : l'action posée, l'objet utilisé, le sujet et le préjudice subi par cette dernière. La valeur ajoutée de ce cadre de définition de la victimisation est que nous avons

élargi la notion de préjudice pour inclure d'autres formes de préjudices comme la perte de temps et l'atteinte à la réputation. Ce cadre a donc permis de définir trois formes de victimisation et, pour chacune d'elles, nous avons utilisé les données de l'ESG 2009 de Statistiques Canada pour analyser les facteurs de risque à la seconde étape (chapitre 5).

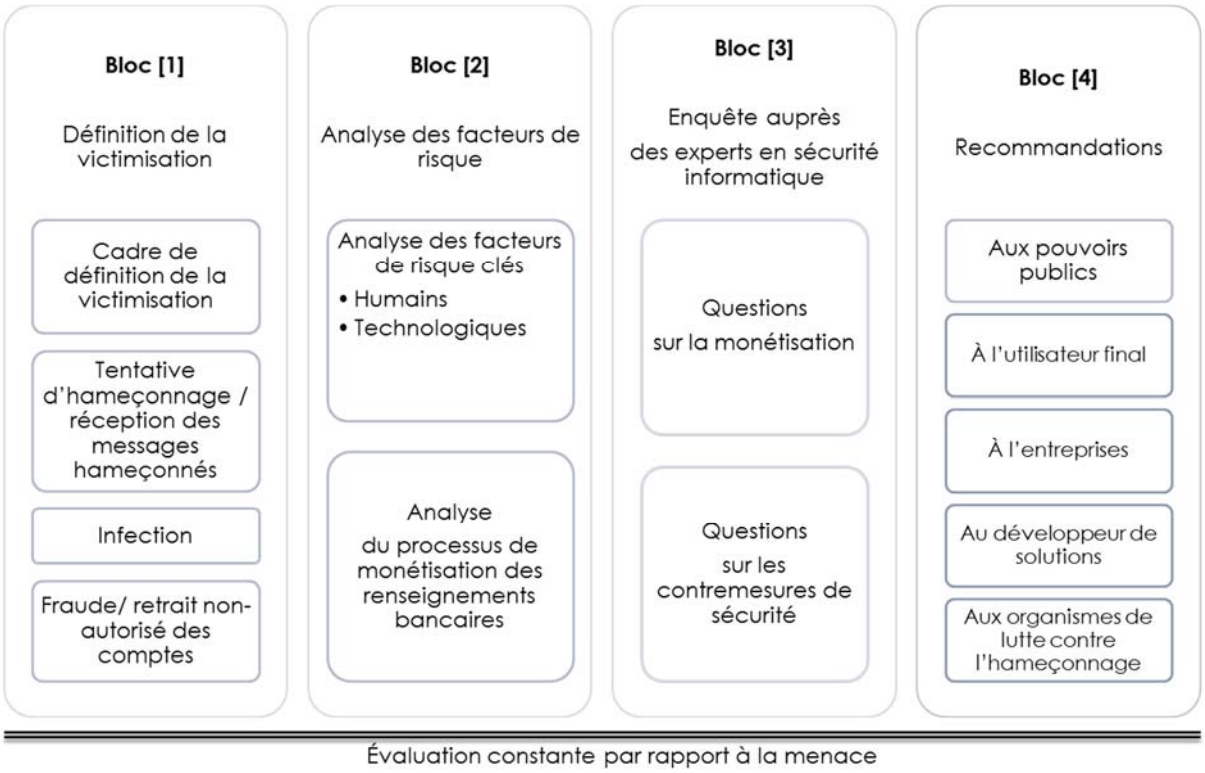


Figure 9.1 : Cadre d'analyse et de réduction de risque d'hameçonnage bancaire proposé

Il ressort de cette analyse que le comportement en ligne de l'internaute est déterminant dans la victimisation. En fait, la fréquence d'utilisation d'internet pour effectuer les achats et les opérations bancaires en ligne est plus prédictible de tentative d'hameçonnage et de fraude que tous les autres facteurs de risque. Pour la victimisation par infection, le facteur de prédiction le plus important est l'utilisation des salons de clavardage suivie, étonnamment, du genre et de l'activité principale de l'internaute. Aussi, afin d'étudier le rapport entre victimisation et l'aversion de l'internaute vis-à-vis du risque, nous avons exploré la notion d'Aléa moral. Les résultats de cette dernière analyse ne permettent ni de tirer de conclusion sur la relation potentielle entre l'aversion vis-à-vis du risque et la victimisation, ni de répondre à notre question de recherche Q2 car nous ne disposions pas de

données pour déterminer les facteurs de risque de la phase de monétisation. Alors, nous avons développé, au chapitre 6, un modèle microéconomique d'équilibre partiel afin de déterminer parmi toutes les variables qui caractérisent le processus de monétisation, lesquelles étaient plus susceptibles de favoriser la monétisation de renseignements. Les résultats de simulation de ce modèle couplés aux avis des experts que nous avons sondés au cours d'une enquête, ont permis de répondre à nos questions de recherche Q2 et Q6 en classifiant les facteurs de risque de victimisation.

La troisième étape de notre approche a consisté à mener une enquête auprès de dix-sept experts en sécurité informatique afin de recueillir leur avis sur les mesures d'amélioration pour atténuer les facteurs de risque que nous avons déterminés à l'étape précédente. L'analyse d'une partie de ces résultats, au chapitre 7, donne des éléments de réponse à notre question Q5. En effet, bien qu'un cadre juridique contraignant visant à favoriser l'échange des listes noires ne soit pas envisageable à court et moyen termes, il est, par exemple, possible de créer des incitatifs fiscaux afin de favoriser la collaboration des acteurs des secteurs public et privé dans la lutte contre l'hameçonnage bancaire. D'autres recommandations du genre sont résumées au Tableau 8.2. L'analyse des autres résultats de l'enquête indique que la réduction de risque lié au taux d'erreurs des filtres anti-hameçonnage et des vulnérabilités des navigateurs est possible si l'on suit les recommandations que nous avons faites à ce sujet (cf. Tableau 8.3 et Tableau 8.4) et qui répondent à nos questions de recherche Q3 et Q4.

La dernière étape de notre approche porte sur les recommandations de mesures pour lutter contre l'hameçonnage. Les recommandations que nous formulons, au chapitre 8, émanent d'une analyse croisée des choix de réponses des experts sondés sur les énoncés issus de la revue de littérature et de notre expérience personnelle d'analyse en sécurité informatique. Nous avons choisi de les regrouper en catégories selon l'auditoire auquel elles s'adressent. Et, nous constatons à la lumière de toutes les recommandations que la mesure à prioriser c'est la sensibilisation et l'éducation de l'utilisateur final. C'est ce dernier qui est le maillon faible de la chaîne, c'est lui qui a tout à perdre, c'est lui qu'il faut sensibiliser en premier.

Ce travail a toutefois certaines limites que nous avons identifiées ci-dessous.

9.3 Limites de la recherche

Ce travail présente plusieurs limites malgré une démarche méthodologique à la fois exploratoire et explicative et bien que nous ayons validé notre modèle théorique avec des données d'une enquête menée auprès d'experts en sécurité informatique.

La principale limite tient à la démarche de modélisation du processus de monétisation. Nous avons fait un travail de modélisation en supposant que le fraudeur agit comme un agent économique rationnel. Or, dans ce milieu, ce n'est pas toujours le cas. Le marché des produits de la cybercriminalité en est un dit « des citrons » (Herley & Florêncio, 2010). C'est un marché où il y a de la contingence. C'est-à-dire que les acteurs ne sont pas toujours rationnels en raison de l'asymétrie de l'information, de leur attitude vis-à-vis du risque et des aléas de ce marché.

La deuxième limite tient au fait que nous avons utilisé des données de deux enquêtes distinctes pour étudier les trois formes de victimisation et ce, en raison des difficultés rencontrées dans la recherche des données relatives à la victimisation par hameçonnage bancaire. Les données de l'enquête ESG 2009 ont permis d'analyser les facteurs de risque de victimisation alors que les avis d'experts ont été utilisés pour valider les résultats du modèle théorique de monétisation. Il aurait été plus logique d'exploiter les données de la même enquête pour à la fois analyser les facteurs de risque de victimisation et étudier les améliorations des contremesures.

La troisième limite est qu'il existe un biais potentiel dans le choix des experts que nous avons recrutés. Ce biais tient au fait que sur les 17 experts, nous avons une disparité de spécialisations (criminologue, cyber-enquêteur, gestionnaire, etc.). Ce qui peut avoir eu un impact sur les résultats en ce sens que la justesse des réponses aux questions peut être fonction du degré de maîtrise par l'expert du sujet auquel réfère l'énoncé.

Une autre limite de cette recherche est le nombre restreint des experts qui ont répondu à cette enquête. Bien qu'une large majorité de ces experts avaient déclaré avoir une longue expérience en sécurité informatique (70% avaient 6 ans et plus) et dans la lutte contre l'hameçonnage (54% avaient 6 ans et plus), la taille de cet échantillon limite la portée de notre recherche.

Ces limites ne sont pas les seuls éléments qui relativisent la portée de ce travail. Il faut y ajouter le fait que la menace change à un rythme effréné, faisant en sorte que la recherche de solutions à l'hameçonnage bancaire reste un défi qui ira croissant et fera l'objet d'un questionnement perpétuel.

9.4 Contributions à la recherche

Plusieurs contributions à l'avancement des connaissances dans la lutte contre l'hameçonnage bancaire peuvent être tirées de cette recherche :

La première est une vaste revue de littérature qui a été réalisée sur le sujet de l'hameçonnage bancaire et qui couvre à la fois, les champs de la sécurité informatique, de la microéconomie et des marchés noirs des produits de la cybercriminalité. Jusqu'ici la revue de littérature des travaux antérieurs se limitait soit à l'hameçonnage, soit aux forums clandestins ou encore à l'étude des modèles microéconomiques des marchés noirs et ne couvrait pas tout le large spectre des activités qui concourent à la fraude bancaire par hameçonnage.

La seconde contribution est le modèle micro-économique que nous avons proposé et qui utilise la théorie du choix rationnel développée en économie pour étudier le processus de monétisation des renseignements bancaires dans le but d'identifier les variables clés sur lesquelles agir si l'on veut perturber ce marché et ses acteurs.

La troisième contribution a été de proposer une méthode d'analyse des facteurs de prédiction de risque d'hameçonnage bancaire selon une perspective centrée sur la victime, puis, de la valider avec un très grand échantillon de répondants (19 422 personnes).

La quatrième contribution est un ensemble de recommandations d'améliorations de mesures de réduction de risque issues des avis des experts que nous avons sondés au cours d'une enquête et de notre propre expérience en sécurité informatique.

La cinquième contribution a été de proposer un cadre de définition de la victimisation par hameçonnage bancaire.

Enfin, il nous a paru intéressant d'apporter une contribution à la compréhension du rôle joué par le risque moral sur la victimisation par hameçonnage.

9.5 Enjeux futurs

Nous savons comment modéliser un processus de monétisation en présumant que le fraudeur agit comme un agent économique rationnel. Il serait intéressant, dans une étude future, d'étudier son comportement en tenant compte de l'asymétrie des informations du marché noir des

renseignements bancaires. Cela suppose que des données empiriques soient colligées dans ces forums et auprès des banques et analysées à cette fin.

La seconde piste de réflexion concerne la recherche des véritables causes humaines du risque d'hameçonnage bancaires. Nous avons identifié au chapitre cinq les facteurs humains prédicteurs du risque de victimisation. Par exemple, nous avons trouvé que le revenu ou le genre augmenterait le risque de tentative d'hameçonnage, toutes choses égales par ailleurs. Toutefois, en poussant la réflexion plus loin, on arrive à l'idée que ce n'est peut-être pas tant le genre qui influence la victimisation mais les prédicteurs comme la sensibilisation aux enjeux de sécurité ou le profil de risque de l'individu. Or, les données de l'enquête ESG 2009 ne permettent pas d'étudier ces deux prédicteurs. Nous pensons qu'une meilleure compréhension des différences sociodémographiques dans le risque de victimisation pourrait permettre aux praticiens, aux chercheurs et aux décideurs de mieux concevoir les interventions dans la lutte contre l'hameçonnage bancaire. Il serait donc important d'étudier, dans une étude future, les causes sous-jacentes de ces différences sociodémographiques.

Enfin, il y a le concept du risque moral appliqué au domaine de la sécurité informatique que nous avons étudié rapidement dans ce travail et que nous suspectons d'être probablement un incitatif à l'adoption de comportement à risque. Une étude future qui utiliserait des données spécifiques sur le sujet permettrait probablement de comprendre l'adoption de certains comportements à risque.

En terminant, cette étude et les recommandations que nous avons faites donnent un cliché instantané de ce qui est en réalité un processus vivant et par le fait même contradictoire. Chaque nouvelle menace nous emmène à questionner nos approches de défense afin d'y intégrer la nouvelle donne avec pour toile de fond la victime.

BIBLIOGRAPHIE

Abad, C. (2005). The economy of phishing: A survey of the operations of the phishing market. *First Monday, 10*(9).

ABC. (2017). Association des banquiers Canadiens : Les Canadiens et leurs services bancaires. Retrieved from http://www.cba.ca/technology-and-banking

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for Cybercrime Tools and Stolen Data.

Abraham, L. B., Morn, M. P., & Vollman, A. (2010). Women on the web: How women are shaping the internet. *Comscore Inc*.

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). *Predicting phishing websites using classification mining techniques with experimental case studies.* Paper presented at the Information Technology: New Generations (ITNG), 2010 Seventh International Conference on.

Acar, T., Belenkiy, M., & Küpçü, A. (2013). Single password authentication. *Computer Networks, 57*(13), 2597-2614.

ACCC. (2017). Australian Competition & Consumer Commission (ACCC). Retrieved from http://www.scamwatch.gov.au/content/index.phtml/itemId/693900

Adida, B., Hohenberger, S., & Rivest, R. L. (2005). *Separable identity-based ring signatures: Theoretical foundations for fighting phishing attacks.* Paper presented at the Proceedings of DIMACS Workshop on Theft in E-Commerce: Content, Identity, and Service.

Affaires. (2014). Les PME de plus en plus visées par l'hameçonnage ciblé. Retrieved from http://www.lesaffaires.com/techno/technologie-de-l-information/l-hameconnage-cible-vise-de-plus-en-plus-les-pme/568003

Al-Hamar, M. K. (2010). *Reducing the risk of e-mail phishing in the state of Qatar through an effective awareness framework.* © Mariam Khalid Al-Hamar,

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. doi:http://dx.doi.org/10.1016/j.cose.2017.04.006

Alkhozae, M. G., & Batarfi, O. A. (2011). Phishing websites detection based on phishing characteristics in the webpage source code. *International Journal of Information and Communication Technology Research, 1*(6).

Alseadoon, I. M. A. (2014). *The impact of users' characteristics on their ability to detect phishing emails.* Queensland University of Technology,

Anderson, R. (2001). *Why information security is hard-an economic perspective.* Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual.

Anderson, R. (2008). Information security economics-and beyond. *Deontic Logic in Computer Science*, 49-49.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., . . . Savage, S. (2012). *Measuring the Cost of Cybercrime.* Paper presented at the 11th Annual Workshop on the Economics of Information Security - WEIS 2012, , Berlin, Germany, 25-26 June 2012.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610.

APWG. (2016). *Phishing Activity Trends Report, 4th Quarter 2015*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2015.pdf

APWG. (2017). *Phishing Activity Trends Report, 4th Quarter 2016*. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Armano, G. (2016). Real-Time Client-Side Phishing Prevention.

Arnaques, S. (2015). Le phishing. Retrieved from https://wiki.signal-arnaques.com/arnaque-type/phishing

Aston, M., McCombie, S., Reardon, B., & Watters, P. (2009). *A preliminary profiling of internet money mules: An australian perspective.* Paper presented at the Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on.

Aublet-Cuvelier, L., & da Cruz, J.-M. M. (2011). Les défis et les opportunités techniques du fonctionnement d'un service antispam mutualisé.

Austin, C. F., Wan, X., & Wright, A. (2013). Two-factor authentication. In: Google Patents.

Aycock, J. (2007). *A design for an anti-spear-phishing system.* Paper presented at the Virus Bulletin Conference.

Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law & Security Review, 23*(3), 276-281.

Basnet, R. B., Mukkamala, S., & Sung, A. H. (2008). Detection of Phishing Attacks: A Machine Learning Approach. *Soft Computing Applications in Industry, 226*, 373-383.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *The Journal of Political Economy, 76*(2), 169-217.

Becker, G. S. (1974). Crime and punishment: An economic approach. In *Essays in the Economics of Crime and Punishment* (pp. 1-54): UMI.

Belani, R., Higbee, A., & Greaux, S. (2016a). Methods and systems for preventing malicious use of phishing simulation records. In: Google Patents.

Belani, R., Higbee, A., & Greaux, S. (2016b). Performance benchmarking for simulated phishing attacks. In: Google Patents.

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of computer security, 18*(1), 7-35.

Bouchard, L. (2017). *Cyber sécurité : le rôle du CA.* Retrieved from https://www.cas.ulaval.ca/files/content/sites/college/files/documents/reseau-asc/programme-perfectionnement/seminaire-16mai2017/presentation-seminaire-cybersecurite-16mai2017-VF.pdf

Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement. *Rutgers Computer & Tech. LJ, 30*, 1.

Brenner, S. W. (2006). Defining cybercrime: A review of state and federal law. *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 13-94.

CAFC. (2015). Rapport statistique trimestriel : avril à juin 2015 - Activités de fraude par marketing de masse et de vol d'identité. Retrieved from http://www.antifraudcentre-centreantifraude.ca/reports-rapports/2015/qt2-fra.htm

CAFC. (2017). Mois de la prévention de la fraude. Retrieved from http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03662.html

Cárdenas, A. A., Radosavac, S., Grossklags, J., Chuang, J., & Hoofnagle, C. (2010). *An economic map of cybercrime.* Paper presented at the The 37th Research Conference on Communication, Information and Internet Policy (TPRC). George Mason University Law School, Arlington, VA.

Casola, L. (2007). Black Markets: Empirical studies into the economic behaviour of the black market consumer.

Chan, T. (2004). HK$660,000 stolen in e-bank scam. *China Daily HK Edition*. Retrieved from http://www.chinadaily.com.cn/english/doc/2004-10/08/content_380368.htm

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). *Phishing email detection based on structural properties*. Paper presented at the NYS Cyber Security Conference.

Chassigneux, C. (2003). La protection des informations à caractère personnel.

Chaudhary, S. (2016). The Use of Usable Security and Security Education to Fight Phishing Attacks.

CHAWKI, M. (2006). Phishing in Cyberspace: Issues and Solutions. Retrieved from http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions/

Chen, T.-C., Dick, S., & Miller, J. (2010). Detecting visually similar web pages: Application to phishing detection. *ACM Transactions on Internet Technology (TOIT), 10*(2), 5.

Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems, 50*(4), 662-672.

Chen, Y.-S., Yu, Y.-H., Liu, H.-S., & Wang, P.-C. (2014). *Detect phishing by checking content consistency*. Paper presented at the Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on.

Chhikara, J., Dahiya, R., Garg, N., & Rani, M. (2013). Phishing & anti-phishing techniques: Case study. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5).

Choi, K.-s., Scott, T., & LeClair, D. P. (2016). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology*.

Choi, K., Lee, J.-l., & Chun, Y.-t. (2017). Voice phishing fraud and its modus operandi. *Security Journal, 30*(2), 454-466.

Christin, N., Yanagihara, S. S., & Kamataki, K. (2010). *Dissecting one click frauds*. Paper presented at the Proceedings of the 17th ACM conference on Computer and communications security.

Clearinghouse. (2003). Watch Out for "Phishing" Emails Attempting to Capture Your Personal Information. Retrieved from https://www.privacyrights.org/ar/phishing.htm

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Comesongsri, V. (2010). *Motivation for the avoidance of phishing threat*: The University of Memphis.

Cooley, S., & Sobel, W. E. (2012). Anti-phishing early warning system based on end user data submission statistics. In: Google Patents.

Corr, M. (2015). *The underground economy of organized cybercrime*. Utica College,

Costăchescu, A. (2012). Comment créer une terminologie?(Lexique de l'informatique). *Résumé, 141*, 155.

Cressey, D. R. (1986). Why managers commit fraud. *Australian & New Zealand Journal of Criminology, 19*(4), 195-209.

Cymru, T. (2006). The underground economy: priceless. In: login.

Dan, G. (2015). *Aspects of Modeling Fraud Prevention of Online Financial Services*. KTH Royal Institute of Technology,

Darwish, A., El Zarka, A., & Aloul, F. (2012). *Towards understanding phishing victims' profile.* Paper presented at the Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on.

Daubrée, C. (1994). Analyse micro-économique de la contrebande et de la fraude documentaire, avec références aux économies africaines. *Revue économique*, 165-192.

Deffains, B., & Kopp, P. (2014). Criminalité financière et blanchiment: le choix des armes.

Del Castillo, M. D., Iglesias, A., & Serrano, J. I. (2007). *Detecting phishing e-mails by heterogeneous classification.* Paper presented at the International Conference on Intelligent Data Engineering and Automated Learning.

Delgado, O., Fuster-Sabater, A., & Sierra, J. (2008). *Analysis of new threats to online banking authentication schemes.* Paper presented at the X Spanish Meeting on Cryptology and Information Security-RECSI.

Dembe, A., & Boden, L. (2000). Moral hazard: a question of morality? *New solutions: a journal of environmental and occupational health policy: NS, 10*(3), 257-279.

Deuss, K. (2016). *Mécanismes de social engineering (phishing).* Haute école de gestion de Genève,

Dhamija, R., & Tygar, J. D. (2005). Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Dinna, N., Leau, Y., Habeeb, S., & Yanti, A. (2008). Managing legal, consumers and commerce risks in phishing. *International Journal of Human and Social Sciences, 3*(5).

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Dong, X., Clark, J. A., & Jacob, J. L. (2008). *User behaviour based phishing websites detection.* Paper presented at the Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on.

Douglass, D. B. (2009). An examination of the fraud liability shift in consumer card-based payment systems. *Economic Perspectives*(QI), 43-49.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). *Behavioral response to phishing risk.* Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Dupont, B. (2013). La coévolution de la technologie et de la délinquance: Quelques intuitions criminologiques. *International Annals of Criminology, 51*(1-2), 39-56.

Eisen, O. (2009). In-session phishing and knowing your enemy. *Network Security, 2009*(3), 8-11.

Emigh, A. (2005). *Online identity theft: Phishing technology, chokepoints and countermeasures*: Identity Theft Technology Council.

Emigh, A. (2006). The crimeware landscape: Malware, phishing, identity theft and beyond. *Journal of Digital Forensic Practice, 1*(3), 245-260.

Fang, X., & Zhan, J. (2010). *Online banking authentication using mobile phones.* Paper presented at the Future Information Technology (FutureTech), 2010 5th International Conference on.

Felix, J., & Hauck, C. (1987). System security: a hacker's perspective. *Interex Proceedings, 1*, 6-6.

Felt, A. P., & Wagner, D. (2011). *Phishing on mobile devices*: na.

Feng, Q., Tseng, K.-K., Pan, J.-S., Cheng, P., & Chen, C. (2011). *New anti-phishing method with two types of passwords in OpenID system.* Paper presented at the Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on.

Fette, I., Sadeh, N., & Tomasic, A. (2007). *Learning to detect phishing emails.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Field, S. A., Cram, E. E., & Gonzalez, J. F. (2016). Providing multi-level password and phishing protection. In: Google Patents.

Florencio, D., & Herley, C. (2012). Is everything we know about password stealing wrong? *IEEE Security & Privacy, 10*(6), 63-69.

Florêncio, D., & Herley, C. (2010). *Phishing and money mules.* Paper presented at the Information Forensics and Security (WIFS), 2010 IEEE International Workshop on.

Fossi, M., Johnson, E., Turner, D., Mack, T., Blackbird, J., McKinney, D., . . . Gough, J. (2008). Symantec report on the underground economy. *Symantec Corporation*.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants.* Paper presented at the ACM conference on Computer and communications security.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security, 27*(7–8), 235-240. doi:http://dx.doi.org/10.1016/j.cose.2008.01.001

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in online social networks. *IEEE Internet Computing, 15*(4), 56-63.

Garfinkel, S., & Cranor, L. (2005). What is Phishing (Or, How to Fight Phishing at the User-Interface Level). In: O'Reilly Network, downloaded from www. oreillynet. com/Ipt/a/6274.

Gaspareniene, L., & Remeikiene, R. (2015). Digital shadow economy: A critical review of the literature. *Mediterranean Journal of Social Sciences, 6*(6 S5), 402.

Gastellier-Prevost, S. (2011). *Vers une détection des attaques de phishing et pharming côté client.* Institut National des Télécommunications,

GC, A. (2013). Credit Card Security.

Gordon, L., & Loeb, M. (2004). The economics of information security investment. *Economics of information security*, 105-125.

Gouda, M. G., Liu, A. X., Leung, L. M., & Alam, M. A. (2007). SPP: An anti-phishing single password protocol. *Computer Networks, 51*(13), 3715-3726.

Graham, R., & Triplett, R. (2016). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, 1-12.

Granova, A., & Eloff, J. (2005). A legal overview of phishing. *Computer Fraud & Security, 2005*(7), 6-11.

GReAT. (2013). "Red October" Diplomatic Cyber Attacks Investigation. Retrieved from https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

Griffiths, M. (2003). Online identity fraud. *Justice of the Peace, 167*, 724-726.

Gupta, D. S., Tanbeer, S. K., & Mohandas, R. (2017). System and method for detecting phishing webpages. In: Google Patents.

Halderman, J. A., Waters, B., & Felten, E. W. (2005). *A convenient method for securely managing passwords.* Paper presented at the Proceedings of the 14th international conference on World Wide Web.

Hamid, A., & Rahmi, I. (2015). *Phishing detection and traceback mechanism*. Retrieved from

Hardt, D. C., & Grennan, K. (2008). Internet Identity Manager. In: US Patent 20,080,071,808.

Hartung, D., & Busch, C. (2010). *Biometric transaction authentication protocol.* Paper presented at the Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on.

He, M., Horng, S.-J., Fan, P., Khan, M. K., Run, R.-S., Lai, J.-L., . . . Sutanto, A. (2011). An efficient phishing webpage detector. *Expert Systems with Applications, 38*(10), 12018-12027.

Herley, C. (2014). Security, cybercrime, and scale. *Communications of the ACM, 57*(9), 64-71.

Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In *Economics of Information Security and Privacy* (pp. 33-53): Springer.

Higbee, A., Belani, R., & Greaux, S. (2013). Simulated phishing attack with sequential messages. In: US Patent 8,615,807.

Higbee, A., Belani, R., & Greaux, S. (2014). Collaborative phishing attack detection. In: Google Patents.

Higbee, A., Belani, R., & Greaux, S. (2016). Collaborative phishing attack detection. In: Google Patents.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19.

Hisamatsu, A., Pishva, D., & Nishantha, G. (2010). *Online banking and modern approaches toward its enhanced security.* Paper presented at the Advanced Communication Technology (ICACT), 2010 The 12th International Conference on.

Holt, T. J. (2013a). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165-177.

Holt, T. J. (2013b). Exploring the social organisation and structure of stolen data markets. *Global Crime, 14*(2-3), 155-174.

Holt, T. J., Chua, Y.-T., & Smirnova, O. (2013). *An exploration of the factors affecting the advertised price for stolen data.* Paper presented at the eCrime Researchers Summit (eCRS), 2013.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies, 23*(1), 33-50.

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. *Computer Security–ESORICS 2009*, 1-18.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Huang, C.-Y., Ma, S.-P., & Chen, K.-T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications, 34*(4), 1292-1301.

Huang, H., Tan, J., & Liu, L. (2009). *Countermeasure Techniques for Deceptive Phishing Attack.* Paper presented at the 2009 International Conference on New Trends in Information and Service Science.

Hutchings, A., & Hayes, H. (2008). Routine activity theory and phishing victimisation: Who gets caught in the net. *Current Issues Crim. Just., 20*, 433.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime, 18*(1), 11-30.

IC3. (2017). The Internet Crime Complaint Center (IC3). Retrieved from http://www.ic3.gov/default.aspx

Islam, C. S. (2017). Phishing Attack Detection Using Taxonomy Model. *Australian Academy of Business and Economics Review, 2*(1), 22-39.

Jaeger, J.-M. D. (2016). Des pirates volent 72 millions de dollars à une plateforme de Bitcoin. Retrieved from http://www.lefigaro.fr/secteur/high-tech/2016/08/03/32001-20160803ARTFIG00143-des-pirates-volent-72-millions-de-dollars-a-une-plateforme-de-bitcoin.php

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Jammalamadaka, R. C., Mehrotra, S., & Venkatasubramanian, N. (2005). *Pvault: a client server system providing mobile access to personal data.* Paper presented at the Proceedings of the 2005 ACM workshop on Storage security and survivability.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology, 32*(6), 584-593.

Kamble, S., Malshikare, A., Gargund, P., & Bhagwat, C. (2015). Securing internet banking from phishing attack. *Multidisciplinary Journal of Research in Engineering and Technology, 2*(3), 562-567.

Kay, F. (2017). *Not Everyone Is a Target: An Analysis of Online Identity Crime Victimization Using Routine Activities Theory.*

Kerstein, P. L. (2005). How can we stop phishing and pharming scams? *CSO Update*.

Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., Schrittwieser, S., Sinha, M., & Weippl, E. (2010). *QR code security.* Paper presented at the Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia.

Kim, S.-H., Choi, D., Jin, S.-H., & Lee, S.-H. (2013). *Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack.* Paper presented at the Proceedings of the 2013 ACM workshop on Digital identity management.

Kim, S., Kang, J.-y., & Kim, Y. (2015). Countermeasures against phishing/pharming via portal site for general users. *The Journal of Korean Institute of Communications and Information Sciences, 40*(6), 1107-1113.

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal, 49*(5), 554-561.

Kitchen, P. (2006). Examen du lien entre la criminalité et la situation socio-économique à Ottawa et à Saskatoon: Analyse géographique à petite échelle.

Kopp, P. (1992). Les analyses formelles des marchés de la drogue. *Revue Tiers Monde*, 565-579.

Kopp, P. (2002). Analyse économique de la délinquance financière.

Kopp, P. (2003). Criminalité d'affaires: analyse économique de l'efficacité des sanctions pénales.

Korolov, M. (2015). Phishing is a $3.7-million annual cost for average large company. Retrieved from http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html

Kovach, S., & Ruggiero, W. V. (2011). *Online banking fraud detection based on local and global behavior.* Paper presented at the Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France.

KPMG. (2013). Global profiles of the fraudster. White-collar crime – present and future.

Krebs, B. (2007). Shadowy Russian Firm Seen as Conduit for Cybercrime. Retrieved from http://www.washingtonpost.com/wp-dyn/content/story/2007/10/12/ST2007101202661.html?hpid=topnews

Krebs, B. (2010). Following the Money, ePassporte Edition. Retrieved from http://krebsonsecurity.com/2010/09/following-the-money-epassporte-edition/

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847. doi:http://dx.doi.org/10.1016/j.cose.2010.08.001

Kruck, G. P., & Kruck, S. (2006). Spoofing–a look at an evolving threat. *Journal of Computer Information Systems, 47*(1), 95-100.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE, 4*(1), 33-39.

Kshetri, N. (2010). Simple economics of cybercrime and the vicious circle. In *The global cybercrime industry* (pp. 35-55): Springer.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). *Getting users to pay attention to anti-phishing education: evaluation of retention and transfer*. Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*(2), 7.

Lalonde Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). *A clinical study of risk factors related to malware infections.* Paper presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.

Lao, G., & Wang, X. (2010). *Study of Security Mechanisms in Personal Internet Banking-Take China Merchants Bank as an Example.* Paper presented at the Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on.

Larcom, G., & Elbirt, A. (2006). Gone phishing. *IEEE Technology and Society Magazine, 25*(3), 52-55.

Larson, J. S. (2010). Enforcing intellectual property rights to deter phishing. *Intellectual Property & Technology Law Journal, 22*(1), 1.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(1), 9.

Legaldictionary. (2017). Bank Fraud. Retrieved from https://legaldictionary.net/bank-fraud/

Lerner, A., Saxena, A., Ouimet, K., Turley, B., Vance, A., Kohno, T., & Roesner, F. (2015). *Analyzing the use of quick response codes in the wild.* Paper presented at the Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704-722.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Leung, C.-M. (2009). *Visual security is feeble for anti-phishing.* Paper presented at the Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on.

Lévesque, F. L., Davis, C. R., & Fernandez, J. M. Evaluating antivirus products with field studies. *Proceedings of the 22th Virus Bulletin International Conference*.

Levin, K., Cashore, B., Bernstein, S., & Auld, G. (2012). Overcoming the tragedy of super wicked problems: constraining our future selves to ameliorate global climate change. *Policy sciences, 45*(2), 123-152.

Lewis, J. L. (2011). *Exploring the Identity-Theft Prevention Efforts of Consumers in the United States*: ERIC.

Li, X., Hu, H., Bai, G., Jia, Y., Liang, Z., & Saxena, P. (2014). *Droidvault: A trusted data vault for android devices.* Paper presented at the Engineering of Complex Computer Systems (ICECCS), 2014 19th International Conference on.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers*, 1-13.

Lillian Ablon, Martin C. Libicki, & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaa*. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Liu, B. H., Hsu, Y. P., & Ke, W. C. (2014). Virus infection control in online social networks based on probabilistic communities. *International Journal of Communication Systems, 27*(12), 4481-4491. doi:10.1002/dac.2630

Lovet, G. (2009). *Fighting Cybercrime: Technical, juridical and ethical challenges.* Paper presented at the Virus Bulletin Conference.

Luhmann, N. (2001). Confiance et familiarite. *Réseaux*(4), 15-35.

Lunde, R., Franklin, S., Lulich, D., & Pierson, G. (2007). Detecting and preventing man-in-the-middle phishing attacks. In: Google Patents.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security, 38*, 28-38.

Ma, J., Saul, L. K., Savage, S., & Voelker, G. M. (2009). *Beyond blacklists: learning to detect malicious web sites from suspicious URLs.* Paper presented at the Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining.

Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009). *Detecting phishing emails using hybrid features.* Paper presented at the Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on.

Ma, Q. (2013a). The process and characteristics of phishing attacks-A small international trading company case study. *Journal of Technology Research, 4*, 1.

Ma, Q. (2013b). The process and characteristics of phishing attacks: A small international trading company case study. *Journal of Technology Research, 4*, 1.

Maggi, F. (2010). *Are the con artists back? a preliminary analysis of modern phone frauds.* Paper presented at the Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on.

Maruatona, O. (2013). *Internet Banking Fraud Detection Using Prudent Analysis.* University of Ballarat,

Mastrobuoni, G. (2011). Optimal criminal behavior and the disutility of jail: Theory and evidence on bank robberies. *Carlo Alberto Notebooks, 220*.

Maurer, M.-E. (2014). *Counteracting phishing through HCI: detecting attacks and warning users.* München, Ludwig-Maximilians-Universität, Diss., 2014,

Mayhorn, C. B., Murphy-Hill, E., Zielinska, O. A., & Welk, A. K. (2015). The social engineering behind phishing. *The next wave, 21*(2).

McGrath, D. K., Kalafut, A., & Gupta, M. (2009). Phishing infrastructure fluxes all the way. *IEEE Security & Privacy, 7*(5).

McNealy, J. E. (2008). Angling for phishers: Legislative responses to deceptive e-mail. *Comm. L. & Pol'y, 13*(2), 275-300.

Mell, A. (2012). Reputation in the Market for Stolen Data. *Discussion Series Paper, Department of Economics, University of Oxford*.

Mihai, I.-C. (2012). Overview on Phishing Attacks. *Int'l J. Info. Sec. & Cybercrime, 1*, 61.

Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. *Retrieved December, 1*(2007), 3.3.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012). *An assessment of features related to phishing websites using an automated technique.* Paper presented at the Internet Technology And Secured Transactions, 2012 International Conference for.

Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime Criminal Law and Criminal Justice, 13*(3), 435.

Moore, T., & Anderson, R. (2011). Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. *Harvard Computer Science Technical Reports for 2011*.

Moore, T., & Clayton, R. (2007). *Examining the impact of website take-down on phishing.* Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Moore, T., & Clayton, R. (2008). *The consequence of non-cooperation in the fight against phishing.* Paper presented at the eCrime Researchers Summit, 2008.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. *The Journal of Economic Perspectives*, 3-20.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). *An analysis of underground forums.* Paper presented at the Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

Muchang, Y., Trushchenkova, S., Somaiya, M., Jabbara, M., & Badley, D. (2015). Browser extension with additional capabilities. In: Google Patents.

Murdoch, S. J., & Anderson, R. (2010). *Verified by visa and mastercard securecode: or, how not to design authentication.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Murphy, J. M. (2005). *The water is wide: network security at Kenyon College, 1995-2005.* Paper presented at the Proceedings of the 33rd annual ACM SIGUCCS conference on User services.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773.

Nguyen, L. A. T., To, B. L., Nguyen, H. K., & Nguyen, M. H. (2013). *Detecting phishing web sites: A heuristic url-based approach.* Paper presented at the Advanced Technologies for Communications (ATC), 2013 International Conference on.

Northfield, V. (1996). Introduction to Computer Crime.

Nuha, A. Z., & Asadullah, S. (2013). Towards Quick Response and Secure Online Banking Transactions Using Data Compression and Cryptography. *Proc. of the Second Intl. Conference on Advances in Information Technology —AIT 2013*, 978-981.

Obied, A., & Alhajj, R. (2009). Fraudulent and malicious sites on the web. *Applied intelligence, 30*(2), 112-120.

Odabas, M., Holt, T. J., & Breiger, R. L. (2017). Governance in Online Stolen Data Markets. *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*, 87.

OpenDNS, L. (2016). PhishTank: An anti-phishing site. *Online: https://www. phishtank. com*.

Otrok, H., Mizouni, R., & Bentahar, J. (2014). *Mobile phishing attack for android platform*. Paper presented at the Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on.

Palande, G., Jadhav, S., Malwade, A., & Baj, S. (2014). An Enhanced Anti-Phishing FrameworkBased on VisualCryptography.

Perreault, S. Self-reported Internet victimization in Canada, 2009. *Juristat, 3*, 85-002.

Perreault, S. (2011). Les incidents autodéclarés de victimisation sur Internet au Canada, 2009. *Juristat. Statistique Canada: Ottawa*.

Perreault, S. (2013). Les incidents autodéclarés de victimisation sur Internet au Canada, 2009. Retrieved from http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-fra.htm

Perreault, S., & Brennan, S. (2010). La victimisation criminelle au Canada, 2009. *Juristat, 30*(2), 85-002.

Peterson. (2011). Email Attacks: This Time It's Personal. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf

Phishing-Initiative. (2017). Phishing Initiative. Retrieved from http://www.phishing-initiative.com/

Phishlabs. (2017). *2017 Phishing Trends and Intelligence Report: Hacking the Human*. Retrieved from https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf

PhishMe. (2016). *PhishMe Q1 2016 Malware Review*. Retrieved from https://phishme.com/project/phishme-q1-2016-malware-review/

Pinguelo, F. M., & Muller, B. W. (2011). Virtual crimes–real damages: A primer on cybercrimes in the united states and efforts to combat cybercriminals.

Polinsky, A. M., & Shavell, S. (2007). The theory of public enforcement of law. *Handbook of law and economics, 1*, 403-454.

Prakash, P., Kumar, M., Kompella, R. R., & Gupta, M. (2010). *Phishnet: predictive blacklisting to detect phishing attacks.* Paper presented at the INFOCOM, 2010 Proceedings IEEE.

Premkumar, S., & Narayanan, A. (2012). *New visual Steganography scheme for secure banking application.* Paper presented at the Computing, electronics and electrical technologies (ICCEET), 2012 international conference on.

Proofpoint. (2017). *« Le facteur humain »*. Retrieved from https://www.proofpoint.com/fr/threat-insight/post/exploiting-human-factor-proofpoint-releases-human-factor-2017-report

Purkait, S. (2012). Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security, 20*(5), 382-420.

Raisbeck, F. (November 10, 2006). Gartner: Targeted phishing attacks target the rich. Retrieved from https://www.scmagazine.com/gartner-targeted-phishing-attacks-target-the-rich/article/552427/

Ramsey, D. (2017). Bank Fraud Law and Legal Definition. Retrieved from https://definitions.uslegal.com/b/bank-fraud/

Rémillard, D. (2013). Services bancaires en ligne: un casse-tête pour les fraudeurs. Retrieved from http://www.lapresse.ca/le-soleil/affaires/zone/securite-de-linformation/201310/13/01-4699391-services-bancaires-en-ligne-un-casse-tete-pour-les-fraudeurs.php

Renaudin, K. (2011). *Le spamming et le droit: analyse critique et prospective de la protection juridique des" spammés"*. Université de Grenoble,

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396-411.

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of computer security, 19*(4), 639-668.

Robertson, H. E. (2011). La loi antipourriel du Canada en vigueur dès cette année.

Roy, S., & Venkateswaran, P. (2014). *Online payment system using steganography and visual cryptography.* Paper presented at the Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on.

Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998). *A Bayesian approach to filtering junk e-mail.* Paper presented at the Learning for Text Categorization: Papers from the 1998 workshop.

Saklikar, S., & Saha, S. (2008). *Public key-embedded graphic captchas.* Paper presented at the Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE.

Schneider, J. L. (2005). Stolen-Goods Markets Methods of Disposal. *British Journal of Criminology, 45*(2), 129-140.

Panda security (2011). Le marché noir de la cyber-criminalité révélé par PandaLabs. Retrieved from https://www.globalsecuritymag.fr/Le-marche-noir-de-la-cyber,20110214,21998.html

Shan, X., & Zhuang, J. (2013). Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *European journal of operational research, 228*(1), 262-272.

Sharifi, M., & Siadati, S. H. (2008). *A phishing sites blacklist generator.* Paper presented at the Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions.* Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems.

Shulman, A. (2010). The underground credentials market. *Computer Fraud & Security, 2010*(3), 5-8. doi:http://dx.doi.org/10.1016/S1361-3723(10)70022-1

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior, 60*, 35-43.

Simmons, M. (1995). Recognizing the elements of fraud. *The Fraud Magazine*.

Singh, A. C., Somase, K. P., & Tambre, K. G. (2013). Phishing: A Computer Security Threat. *International Journal of Advance Research in Computer Science and Management Studies, 1*(7).

Smedinghoff, T. (2005). Phishing the legal challenge for business'. *Banking & Financial Services Policy Report, 24*(4), 1-5.

Smyth, S., & Carleton, R. (2011). Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources.

Smyth, S. M. (2014). The Greening of Canadian Cyber Laws: What Environmental Law can Teach and Cyber Law can learn. *International Journal of Cyber Criminology, 8*(2).

Sood, A. K., Bansal, R., & Enbody, R. J. (2013). Cybercrime: Dissecting the State of Underground Enterprise. *Internet Computing, IEEE, 17*(1), 60-68. doi:10.1109/mic.2012.61

Statistique Canada, les incidents autodéclarés de victimisation sur Internet au Canada, 2009.

StatistiqueCanada. (2009). Enquête sociale générale: Victimisation. Retrieved from http://www23.statcan.gc.ca/imdb/p2SV_f.pl?Function=getSurvey&Id=148641

Symantec. (2008). Symantec Report on the Underground Economy XII. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

Symantec. (2014). *Internet Security Threat Report 2014, volume 19*. Retrieved from http://www.symantec.com/fr/ca/security_response/publications/threatreport.jsp

Symantec. (2016). *Internet Security Threat Report*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

The-419-Coalition. (2016). Nigeria - The 419 Coalition Website - We Fight the Nigerian Scam with Education. Retrieved from http://home.rica.net/alphae/419coal/

Thomas, K. (2013). *The role of the underground economy in social network spam and abuse*: University of California, Berkeley.

Thomas, R., & Martin, J. (2006). The underground economy: Priceless.; login:, 31 (6): 7–16. In: December.

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *NCCD news, 41*(1), 54-72.

Trudel, P., Abran, F., & Dupuis, G. (2007). *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*. Retrieved from http://pierretrudel.openum.ca/files/sites/6/2017/03/PourrielCRDP4-4-7.pdf

US-CERT. (2017). Avoiding Social Engineering and Phishing Attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-014

USFTC. (2017). The United States Federal Trade Commission. Retrieved from http://www.ftc.gov/

Utakrit, N. (2012). Security awareness by online banking users in Western Australian of phishing attacks.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Wall, D. S. (2001). Cybercrimes and the Internet. *Crime and the Internet*, 1-17.

Wang, Q., & Qin, Z. (2010). *Stronger user authentication for web browser.* Paper presented at the Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on.

Winder, D. (2014). Hackernomics: the supply and demand of stolen data, botnets and more. *PC Pro, n 235, p 36-40*.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). *Do security toolbars actually prevent phishing attacks?* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Wueest, C. (2015). Underground black market: Thriving trade in stolen data, malware, and attack services. Retrieved from https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+: A feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security (TISSEC), 14*(2), 21.

Yildiz, M., & Göktürk, M. (2010). *Combining Biometric ID Cards and Online Credit Card Transactions.* Paper presented at the Digital Society, 2010. ICDS'10. Fourth International Conference on.

Yucedal, B. (2010). *Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories.* Kent State University,

Yue, C. (2010). *Enhancing web browsing security*: College of William & Mary.

Zhang, H., Liu, G., Chow, T. W., & Liu, W. (2011). Textual and visual content-based anti-phishing: a Bayesian approach. *IEEE Transactions on Neural Networks, 22*(10), 1532-1546.

Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). *Cantina: a content-based approach to detecting phishing web sites.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Zhuang, J., Bier, V. M., & Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *European journal of operational research, 203*(2), 409-418. doi:http://dx.doi.org/10.1016/j.ejor.2009.07.028

ANNEXE A : CLASSIFICATION DES RÉFÉRENCES CONSULTÉES

Tableau A.1 : Liste des thèses de doctorat et mémoires étudiés

N0	Titre de la thèse	Auteurs	Contribution
1.	Motivation for the avoidance of phishing threat	(Comesongsri, 2010)	Le modèle de recherche proposé est capable d'expliquer les intentions de l'utilisateur d'effectuer des protections de phishing recommandées. Le modèle préconise des messages d'intervention qui doivent persuader l'utilisateur de croire que la menace est réelle et pourrait être sévère.
2.	Enhancing web browsing security	(Yue, 2010)	Le travail a proposé une approche pour alimenter de manière transparente un nombre relativement important de faux renseignements dans un site de phishing suspecté. L'idée était de dissimuler les véritables références de la victime, de sorte que les phishers ne sont pas capables d'utiliser la date à leur avantage.
3.	Detecting visually similar web pages: application to phishing detection	(T.-C. Chen, Dick, & Miller, 2010)	Le travail propose une nouvelle approche pour détecter la similitude visuelle entre deux pages web. L'auteur a également testé son système en utilisant les pages web les plus populaires pour examiner sa fonctionnalité pour la situation réelle. Le résultat montre que la précision de la méthode proposée est extrêmement élevée et que les vrais taux positifs et faux positifs ont atteint respectivement 100 et 0,8%.
4.	Reducing the Risk of E-mail Phishing in the State of Qatar through an Effective Awareness Framework	(Al-Hamar, 2010)	Cette recherche tente de réduire le risque de phishing par courrier électronique grâce à la sensibilisation et à l'éducation. Il souligne le problème du phishing par courrier électronique dans l'État du Qatar, l'un des pays en développement le plus rapide du monde et cherche à fournir une solution pour sensibiliser les gens au phishing par courrier électronique en développant un cadre efficace de sensibilisation et d'éducation

Tableau A.1 : Liste des thèses de doctorat et mémoires étudiés (suite)

5.	Exploring the identity-theft prevention efforts of consumers in the United States	(Lewis, 2011)	Cette étude explore comment les consommateurs conceptualisent l'idée de la prévention du vol d'identité. Il détermine les caractéristiques de ceux qui prennent des mesures pour prévenir le vol d'identité et étudie comment la menace de vol d'identité affecte l'échange de consommation.
6.	Security Awareness by Online Banking Users in Western Australian of Phishing Attacks	(Utakrit, 2012)	Étudier les expériences des utilisateurs des banques de l'Australie occidentale dans l'utilisation des services bancaires en ligne. Examiner la relation entre le contexte des utilisateurs de banques de l'Australie occidentale et leur expérience dans l'utilisation de la sécurité bancaire en ligne.
7.	Internet Banking Fraud Detection Using Prudent Analysis	(Maruatona, 2013)	Cette thèse propose, développe et évalue un système à utiliser dans la détection de fraudes bancaires par Internet en utilisant l'analyse Prudence dans un système RDR (Ripple Down Rules). On a montré que les systèmes de RDR prudents présentent des avantages remarquables par rapport aux bases de règles conventionnelles. En outre, la prudence dans les systèmes RDR permet au système de se rendre compte quand un cas actuel dépasse l'expertise du système. Les résultats indiquent qu'un système RDR prudent est une alternative viable dans la détection de la fraude en banque en ligne.
8.	Counteracting phishing through HCI: Detecting Attacks and Warning Users	(Maurer, 2014)	un modèle qui combine la détection de phishing et l'intervention de l'utilisateur et propose des recommandations de développement et d'évaluation pour des systèmes
9.	The impacts of user's characteristics on their ability to detect phishing emails	(Alseadoon, 2014)	Un modèle pour examiner l'ensemble du processus de détection des utilisateurs et identifier les faiblesses de leur comportement. Le modèle met en lumière les trois phases du comportement de détection et de leurs vulnérabilités: la susceptibilité, la confirmation et la réponse.

Tableau A.1 : Liste des thèses de doctorat et mémoires étudiés (suite)

10.	Phishing Detection and Trackback Mechanism	(Hamid & Rahmi, 2015)	Une approche de sélection de fonctionnalité hybride pour une utilisation dans la détection d'une attaque de phishing par courrier électronique est développée. La méthode proposée est basée sur la combinaison d'approches fondées sur le contenu et sur le comportement. Appliquer des techniques de cluster en fonction de l'algorithme de clustering à deux étapes modifiées pour générer le nombre optimal de clusters.
11.	Aspects of Modeling Fraud Prevention of Online Financial Services	(Dan, 2015)	Un outil qui permet de mesurer l'efficacité du processus de réponse aux incidents : arbre de réponse d'incident (IRT). des scénarios supplémentaires pertinents pour la gestion des risques des services financiers en ligne en utilisant les IRT. un modèle complémentaire inspiré des modèles existants utilisés pour mesurer les risques de crédit.
Marché noir des produits de la cybercriminalité			
12.	Black Markets: Empirical studies into the economic behaviour of the black market consumer.	(Casola, 2007)	Examiner les variables qui affectent les consommateurs à l'achat des produits dans des marchés noirs et leurs perceptions de ces marchés. Les résultats indiquent que les participants au prix étaient disposés à payer pour les biens dans un marché noir variaient en fonction de la victime (individuel, organisation ou société), de l'âge et du sexe du participant.
13.	The Role of the Underground Economy in Social Network Spam and Abuse	(K. Thomas, 2013)	Analyse empirique de la largeur et de la profondeur de la gamme des menaces qui visent actuellement les réseaux sociaux en ligne à travers les lentilles de Twitter. Cartographie de l'infrastructure de support qui est essentielle à l'abus de réseau social en ligne, caractérisation des outils et les techniques utilisés pour diffuser du contenu malin et évaluation de profit pour les attaquants impliqués.

Tableau A.1 : Liste des thèses de doctorat et mémoires étudiés (suite et fin)

14.	The underground economy of organized cybercrime	(Corr, 2015)	Examiner l'économie souterraine de la cybercriminalité organisée et de développer une compréhension globale en répondant aux questions suivantes: quelle est la taille approximative de l'économie souterraine associée à ces organisations? Quelles sont ses caractéristiques et comment se rapporte-t-il au système économique légal?

Tableau A.2 : Références classées par sujets

N0	Titre	(Auteur, année)	Sujets couverts				
			Con-cepts	Tech-niques	Marché noir	Contre mesures	Victimi-sation
Articles							
1.	Recognizing the elements of fraud	(Simmons, 1995)					x
2.	Introduction to Computer Crime	(Northfield, 1996)	x				
3.	Online Identity fraud	(Griffiths, 2003)				x	x
4.	System security: a hacker's perspective	(Felix & Hauck, 1987)		x			
5.	Why information security is hard-an economic perspective	(Anderson, 2001)	x				
6.	Information security economics-and beyond	(Anderson, 2008)	x				
7.	In-session phishing and knowing your enemy	(Eisen, 2009)	x	x			
8.	QR Code Security	(Kieseberg et al., 2010)		x			

Tableau A.2 : Références classées par sujets (suite)

9.	Are the con artists back? a preliminary analysis of modern phone frauds	(Maggi, 2010)		x			
10.	The state of phishing attacks	(Hong, 2012)		x			
11.	The process and characteristics of phishing attacks: A small international trading company case study	(Q. Ma, 2013a)	x	x			
12.	“Red October” Diplomatic Cyber Attacks Investigation	(GReAT, 2013)		x			
13.	hishing & anti-phishing techniques: Case study	(Chhikara et al., 2013)		x		x	
14.	Mobile phishing attack for android platform	(Otrok, Mizouni, & Bentahar, 2014)		x			
15.	Criminalité financière et blanchiment: le choix des armes	(Deffains & Kopp, 2014)	x	x			
16.	Analyzing the use of quick response codes in the wild	(Lerner et al., 2015)	x	x			
17.	Analyse du cadre réglementaire québécois et étranger à l’égard du pourriel, de l’hameçonnage et des logiciels espions.	(Trudel et al., 2007)		x			
18.	Technical trends in phishing attacks	(Milletary & Center, 2005)	x	x			
19.	The crimeware landscape: Malware, phishing, identity theft and beyond	(Emigh, 2006)	x	x			
20.	Spoofing–a look at an evolving threat	(Kruck & Kruck, 2006)		x		x	
21.	Vers une détection des attaques de phishing et pharming côté client	(Gastellier-Prevost, 2011)		x			
22.	Comment créer une terminologie? (Lexique de l’informatique)	(Costăchescu, 2012)	x	x			

Tableau A.2 : Références classées par sujets (suite)

23.	Achieving a consensual definition of phishing based on a systematic review of the literature.	(Lastdrager, 2014)	x				
24.	Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization.	(E Rutger Leukfeldt, 2014)					x
25.	Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks.	(E Rutger Leukfeldt, Kleemans, & Stol, 2016)					x
26.	Applying routine activity theory to cybercrime: A theoretical and empirical analysis.	(Eric Rutger Leukfeldt & Yar, 2016)	x	x			x
27.	Phishing Attack Detection Using Taxonomy Model.	(Islam, 2017)		x			
28.	Phishing environments, techniques, and countermeasures: A survey.	(Aleroud & Zhou, 2017)		x			
29.	Phishing Attack Detection Using Taxonomy Model.	(K. Choi et al., 2017)		x			
30.	Crime and Punishment: An Economic Approach	(Becker, 1968)			x		
31.	Criminalité d'affaires: analyse économique de l'efficacité des sanctions pénales	(Kopp, 2003)			x		
32.	Toward a criminal law for cyberspace: A new model of law enforcement	(Brenner, 2004)			x		
33.	The economics of information security investment.	(Gordon & Loeb, 2004)			x		
34.	Stolen-Goods Markets Methods of Disposal	(Schneider, 2005)			x		
35.	The simple economics of cybercrimes	(Kshetri, 2006)			x		

Tableau A.2 : Références classées par sujets (suite)

36.	The theory of public enforcement of law	(Polinsky & Shavell, 2007)			x		
37.	A legal overview of phishing	(Granova & Eloff, 2005)			x		
38.	The underground economy: priceless	(Cymru, 2006)			x		
39.	The underground economy: Priceless.; login:, 31 (6): 7–16	(R. Thomas & Martin, 2006)			x		
40.	Social phishing	(Jagatic et al., 2007)			x		
41.	An inquiry into the nature and causes of the wealth of Internet miscreants	(Franklin et al., 2007)			x		
42.	Detection of Phishing Attacks: A Machine Learning Approach.	(Basnet, Mukkamala, & Sung, 2008)			x		
43.	Symantec report on the underground economy	(Fossi et al., 2008)			x		
44.	Learning more about the underground economy: A case-study of keyloggers and dropzones.	(Holz, Engelberth, & Freiling, 2009)			x		
45.	The Economics of Online Crime	(Tyler Moore et al., 2009)			x		
46.	A preliminary profiling of Internet money mules: An Australian perspective	(Aston et al., 2009)			x		
47.	Following the Money, ePassporte Edition	(Krebs, 2010)			x		
48.	Dissecting one click frauds	(Christin, Yanagihara, & Kamataki, 2010)			x		

Tableau A.2 : Références classées par sujets (suite)

49.	An economic map of cybercrime	(Cárdenas et al., 2010)			x		
50.	Phishing and money mules	(Florêncio & Herley, 2010)			x		
51.	Exploring stolen data markets online: products and market forces	(Holt & Lampke, 2010)			x		
52.	The underground credentials market	(Shulman, 2010)			x		
53.	Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy	(Herley & Florêncio, 2010)			x		
54.	An analysis of underground forums	(Motoyama et al., 2011)			x		
55.	Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research	(T. Moore & Anderson, 2011)			x		
56.	Le marché noir de la cyber-criminalité révélé par PandaLabs	(Panda, 2011)			x		
57.	Optimal criminal behavior and the disutility of jail: Theory and evidence on bank robberies	(Mastrobuoni, 2011)			x		
58.	Measuring the Cost of Cybercrime	(Anderson et al., 2012)			x		
59.	Reputation in the Market for Stolen Data.	(Mell, 2012)			x		
60.	Is Everything We Know about Password Stealing Wrong?	(Florencio & Herley, 2012)			x		
61.	An exploration of the factors affecting the advertised price for stolen data	(Holt, Chua, & Smirnova, 2013)			x		
62.	Cybercrime: Dissecting the State of Underground Enterprise	(Sood et al., 2013)			x		

Tableau A.2 : Références classées par sujets (suite)

63.	Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack	(S.-H. Kim et al., 2013)			x		
64.	Exploring the social organisation and structure of stolen data markets	(Holt, 2013b)			x		
65.	The role of the underground economy in social network spam and abuse	(K. Thomas, 2013)			x		
66.	Markets for Cybercrime Tools and Stolen Data.	(Ablon, Libicki, & Golay, 2014)			x		
67.	Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaa	(Lillian Ablon et al., 2014)			x		
68.	Hackernomics: the supply and demand of stolen data, botnets and more	(Winder, 2014)			x		
69.	Security, cybercrime, and scale	(Herley, 2014)			x		
70.	The online stolen data market: disruption and intervention approaches.	(Hutchings & Holt, 2017)		x	x		
71.	Digital shadow economy: A critical review of the literature.	(Gaspareniene & Remeikiene, 2015)			x		
72.	Underground black market: Thriving trade in stolen data, malware, and attack services	(Wueest, 2015)			x		
73.	Anti-phishing early warning system based on end user data submission statistics. In: Google Patents	(Cooley & Sobel, 2012)			x		
74.	A Bayesian Approach to Filtering Junk E-Mail	(Sahami et al., 1998)			x		

Tableau A.2 : Références classées par sujets (suite)

75.	La protection des informations à caractère personnel	(Chassigneux, 2003)				x	
76.	Online identity theft: Phishing technology, chokepoints and countermeasures	(Emigh, 2005)				x	
77.	Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks.	(Dhamija & Tygar, 2005)				x	
78.	Pvault: a client server system providing mobile access to personal data	(Jammalamadaka et al., 2005)				x	
79.	A convenient method for securely managing passwords	(Halderman et al., 2005)				x	
80.	Phishing the legal challenge for business'	(Smedinghoff, 2005)				x	
81.	What is Phishing (Or, How to Fight Phishing at the User-Interface Level)	(Garfinkel & Cranor, 2005)				x	
82.	Separable identity-based ring signatures: Theoretical foundations for fighting phishing attacks	(Adida et al., 2005)				x	
83.	Phishing the legal challenge for business'	(Smedinghoff, 2005)				x	
84.	The water is wide: network security at Kenyon College	(Murphy, 2005)				x	
85.	Do security toolbars actually prevent phishing attacks?	(Wu et al., 2006)				x	
86.	Protecting users against phishing attacks	(Kirda & Kruegel, 2006)				x	x
87.	Phishing email detection based on structural properties	(Chandrasekaran, Narayanan, & Upadhyaya, 2006)				x	

Tableau A.2 : Références classées par sujets (suite)

88.	Gone phishing	(Larcom & Elbirt, 2006)				x	
89.	Phishing for user security awareness	(Dodge et al., 2007)				x	
90.	Criminal law tackles computer fraud and misuse	(Bainbridge, 2007)				x	
91.	SPP: An anti-phishing single password protocol	(Gouda et al., 2007)				x	
92.	Cantina: a content-based approach to detecting phishing web sites	(Y. Zhang et al., 2007)				x	
93.	Getting users to pay attention to anti-phishing education: evaluation of retention and transfer	(Kumaraguru et al., 2007)				x	
94.	"Detecting phishing e-mails by heterogeneous classification	(Del Castillo et al., 2007)				x	
95.	Examining the impact of website take-down on phishing	(Tyler Moore & Clayton, 2007)				x	
96.	Detecting and preventing man-in-the-middle phishing attacks	(Lunde et al., 2007)				x	
97.	A phishing sites blacklist generator	(Sharifi & Siadati, 2008)				x	
98.	Angling for phishers: Legislative responses to deceptive e-mail	(McNealy, 2008)				x	
99.	Analysis of new threats to online banking authentication schemes	(Delgado et al., 2008)				x	
100.	Public key-embedded graphic captchas	(Saklikar & Saha, 2008)				x	
101.	Countermeasure Techniques for Deceptive Phishing Attack.	(H. Huang, Tan, & Liu, 2009)				x	
102.	Phishing infrastructure fluxes all the way	(McGrath et al., 2009)				x	
103.	Visual security is feeble for anti-phishing	(Leung, 2009)				x	

Tableau A.2 : Références classées par sujets (suite)

104.	Fighting Cybercrime: Technical, juridical and ethical challenges	(Lovet, 2009)				x	
105.	New filtering approaches for phishing email	(Bergholz et al., 2010)				x	
106.	Teaching Johnny not to fall for phish	(Kumaraguru et al., 2010)				x	
107.	Cantina: a content-based approach to detecting phishing web sites	(Y. Zhang et al., 2007)				x	
108.	Internet Identity Manager	(Hardt & Grennan, 2008)				x	
109.	Beyond blacklists: learning to detect malicious web sites from suspicious URLs	(J. Ma et al., 2009)				x	
110.	User behaviour based phishing websites detection	(Dong et al., 2008)				x	
111.	Stronger user authentication for web browser	(Wang & Qin, 2010)				x	
112.	Enforcing intellectual property rights to deter phishing	(Larson, 2010)				x	
113.	Combining Biometric ID Cards and Online Credit Card Transactions	(Yildiz & Göktürk, 2010)				x	
114.	Predicting phishing websites using classification mining techniques with experimental case studies	(Aburrous et al., 2010)				x	
115.	Phishnet: predictive blacklisting to detect phishing attacks	(Prakash et al., 2010)				x	
116.	Online Banking and Modem Approaches Toward its Enhanced Security	(Hisamatsu et al., 2010)				x	
117.	Online banking authentication using mobile phones	(Fang & Zhan, 2010)				x	
118.	Textual and visual content-based anti-phishing: a Bayesian approach	(H. Zhang et al., 2011)				x	

Tableau A.2 : Références classées par sujets (suite)

119.	Phishing websites detection based on phishing characteristics in the webpage source code	(Alkhozae & Batarfi, 2011)				x	
120.	Online banking fraud detection based on local and global behavior	(Kovach & Ruggiero, 2011)				x	
121.	Automatic analysis of malware behavior using machine learning	(Rieck et al., 2011)				x	
122.	New anti-phishing method with two types of passwords in OpenID system	(Feng et al., 2011)				x	
123.	La loi anti-pourriel du Canada en vigueur dès cette année	(Robertson, 2011)				x	
124.	Using one-time passwords to prevent password phishing attacks	(C.-Y. Huang et al., 2011)				x	
125.	Security issues in online social networks	(Gao et al., 2011)				x	
126.	Virtual crimes–real damages: A primer on cybercrimes in the united states and efforts to combat cybercriminals	(Pinguelo & Muller, 2011)				x	
127.	Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model	(Vishwanath et al., 2011)				x	
128.	Phishing counter measures and their effectiveness–literature review	(Purkait, 2012)				x	
129.	New visual Steganography scheme for secure banking application	(Premkumar & Narayanan, 2012)				x	
130.	An assessment of features related to phishing websites using an automated technique	(Mohammad et al., 2012)				x	

Tableau A.2 : Références classées par sujets (suite)

131.	Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration	(Luo et al., 2013)				x	
132.	Phishing: A Computer Security Threat	(Singh et al., 2013)				x	
133.	Phishing for phishing awareness	(Jansson & von Solms, 2013)				x	
134.	Simulated phishing attack with sequential messages	(Higbee, Belani, & Greaux, 2013)				x	
135.	Towards Quick Response and Secure Online Banking Transactions Using Data Compression and Cryptography	(Nuha & Asadullah, 2013)				x	
136.	Single password authentication	(Acar et al., 2013)				x	
137.	Online payment system using steganography and visual cryptography	(Roy & Venkateswaran, 2014)				x	
138.	An Enhanced Anti-Phishing FrameworkBased on VisualCryptography	(Palande et al., 2014)				x	
139.	Droidvault: A trusted data vault for android devices	(Li et al., 2014)				x	
140.	Detect phishing by checking content consistency	(Y.-S. Chen, Yu, Liu, & Wang, 2014)				x	
141.	Achieving a consensual definition of phishing based on a systematic review of the literature	(Lastdrager, 2014)				x	
142.	Collaborative phishing attack detection	(Higbee, Belani, & Greaux, 2014)				x	

Tableau A.2 : Références classées par sujets (suite)

143.	Legal framework for the enforcement of Cyber law and cyber ethics in Nigeria	(UMEJIAKU, 2015)				x	
144.	Securing Internet banking from phishing attack	(Kamble, Malshikare, Gargund, & Bhagwat, 2015)				x	
145.	Countermeasures against phishing/pharming via portal site for general users	(S. Kim et al., 2015)				x	
146.	PhishTank: An anti-phishing site	(OpenDNS, 2016)				x	
147.	Real-Time Client-Side Phishing Prevention	(Armano, 2016)				x	
148.	Providing multi-level password and phishing protection	(Field, Cram, & Gonzalez, 2016)				x	
149.	The Use of Usable Security and Security Education to Fight Phishing Attacks	(Chaudhary, 2016)				x	
150.	Mécanismes de social engineering (phishing)	(Deuss, 2016)				x	
151.	Performance benchmarking for simulated phishing attacks	(Belani, Higbee, & Greaux, 2016b)				x	
152.	Methods and systems for preventing malicious use of phishing simulation records	(Belani, Higbee, & Greaux, 2016a)				x	
153.	Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests	(Liao, Balasinorwala, & Rao, 2017)				x	
154.	Avoiding Social Engineering and Phishing Attacks	(US-CERT, 2017)				x	
155.	Le Facteur Humain	(Proofpoint, 2017)				x	

Tableau A.2 : Références classées par sujets (suite)

156.	Moral hazard: a question of morality?	(Dembe & Boden, 2000)					x
157.	Developing Policies for Cybercrime: Some Empirical Issues	(Moitra, 2005)					x
158.	Defining cybercrime: A review of state and federal law. Cybercrime:	(Brenner, 2006)					x
159.	The economics of information security	(Anderson & Moore, 2006)					x
160.	An examination of the fraud liability shift in consumer card-based payment systems	(Douglass, 2009)					x
161.	Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions	(Sheng et al., 2010)					x
162.	Why phishing works	(Dhamija et al., 2006)					x
163.	Behavioral response to phishing risk	(Downs, Holbrook, & Cranor, 2007)					x
164.	Social phishing	(Jagatic et al., 2007)					x
165.	Routine activity theory and phishing victimisation: Who gets caught in the net	(Hutchings & Hayes, 2008)					
166.	A routine activity perspective on online victimisation: Results from the Canadian General Social Survey	(Reyns, 2015)					x
167.	The dark side of social networking sites: Understanding phishing risks	(Silic & Back, 2016)					x
168.	Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory	(K.-s. Choi, Scott, & LeClair, 2016)					x

Tableau A.2 : Références classées par sujets (suite et fin)

169.	Not Everyone Is a Target: An Analysis of Online Identity Crime Victimization Using Routine Activities Theory	(Kay, 2017)					x
170.	The economy of phishing: A survey of the operations of the phishing market.	(Abad, 2005)		x	x		
171.	How can we stop phishing and pharming scams	(Kerstein, 2005)				x	
172.	Des pirates volent 72 millions de dollars à une plateforme de Bitcoin	(Jaeger, 2016)					x
173.	Shadowy Russian Firm Seen as Conduit for Cybercrime	(Krebs, 2007)					x
174.	Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories	(Yucedal, 2010)					x
175.	Le marché noir de la cyber-criminalité révélé par PandaLabs	(Panda, 2011)	x	x		x	x
176.	Services bancaires en ligne: un casse-tête pour les fraudeurs	(Rémillard, 2013)					x
177.	Le phishing	(Arnaques, 2015)	x				
178.	Phishing is a $3.7-million annual cost for average large company	(Korolov, 2015)					x
179.	Bank Fraud Law and Legal Definition	(Ramsey, 2017)	x				
180.	Bank Fraud	(Legaldictionary, 2017)	x				

Tableau A.3 : Brevets consultés relativement à l'hameçonnage bancaire

	Brevet cité	**Date de publication**	**Déposant**	**Titre**
1.	US9621566 B2	11 avr. 2017	Adi Labs Incorporated	System and method for detecting phishing webpages
2.	US9325730 B2	26 avr. 2016	PhishMe, Inc.	Collaborative phishing attack detection
3.	US 20150269579	Sep 24, 2015	CA, Inc. (New York, NY)	Controlling e-Commerce authentication based on comparing cardholder information among e-Commerce authentication requests from merchant nodes
4.	US 20150326565	Nov. 12, 2015	Inbay Technologies Inc. (Ottawa, CA)	Method and system for authorizing secure electronic transactions using a security device having a quick response code scanner
5.	US8904168 B1	2 déc. 2014	Aaron Emigh	Email link rewriting with verification of link destination
6.	US20140208406 A1	24 juil. 2014	N-Dimension Solutions Inc.	Two-factor authentication
7.	Appl. # 61605677	Mar 1, 2012	The 41st Parameter, Inc. (Scottsdale, AZ)	Methods and systems for fraud containment
8.	US 20110055047	Mar 3, 2011	Virtual World Computing, LLC (Santa Barbara, CA)	Methods for establishing and using a transaction-specific, browser-specific debit card
9.	US 20150235177	Aug. 20, 2015	Camelot UK Bidco Limited (London, GB)	Online Fraud Solution
10.	US 20100076890	Mar 25, 2010	Paypal, Inc. (San Jose, CA)	GUI-based wallet program for online transactions
11.	CA 2854966	2007-11-08	Digital Envoy, Inc. (USA)	Fraud analyst smart cookie

ANNEXE B : VARIABLES DE L'ENQUÊTE ESG 2009 UTILISÉES DANS CETTE RECHERCHE

Tableau B.1 : Groupes et variables

Groupe Renseignements démographiques										
#	Nom	Libellé	Type	Format	Valide	Non-valide	Codification			
1	AGEGR10	Groupe d'âge du répondant (groupes de 10).	discrète	numeric-1.0	19422	0	1	15 à 24	5	55 à 64 ans
							2	25 à 34	6	65 à 74 ans
							3	35 à 44	7	75 ans et plus
							4	45 à 54		
2	SEX	Sexe du répondant.	discrète	numeric-1.0	19422	0	1	Homme	2	Femme
3	MARSTAT	État matrimonial du répondant.	discrète	numeric-1.0	15111	4311				
Groupe Revenus										
#	Nom	Libellé	Type	Format	Valide	Non-valide	Question			
4	INCM	Revenu personnel annuel du répondant.	discrète	numeric-2.0	16661	2761	Revenu personnel annuel du répondant.			
Groupe Niveau de scolarité du répondant										
#	Nom	Libellé	Type	Format	Valide	Non-valide	Question			
5	EDU10	Le niveau de scolarité le plus élevé atteint par le répondant.	discrète	numeric-2.0	19203	219	Le niveau de scolarité le plus élevé atteint par le répondant. En 10 groupes.			

Tableau B.1 : Groupes et variables (suite)

Groupe Renseignements géographiques							
#	Nom	Libellé	Type	Format	Valide	Non-	Question
6	LUC_RST	Indicateur urbain/rurale.	discrète	numeric-1.0	19422	0	Indicateur urbain/rurale.

Groupe Identité autochtone							
#	Nom	Libellé	Type	Format	Valide	Non- valide	Question
7	AIR_Q110	Êtes-vous un/une Autochtone?	discrète	numeric-1.0	19275	147	Êtes-vous un/une Autochtone (pour cette enquête une personne Autochtone réfère à une personne des Premières Nations [un(e) Indien(ne) de l'Amérique du Nord], un(e) Métis(se) ou un(e) Inuit(e))?

Groupe Langue							
#	Nom	Libellé	Type	Format	Valide	Non-	Question
8	LANHSDC	Langue du ménage du répondant.	discrète	numeric-1.0	19266	156	Langue du ménage du répondant.

Groupe Minorité visible							
#	Nom	Libellé	Type	Format	Valide	Non- valide	Question
9	VISMIN	Statut de minorité visible du répondant.	discrète	numeric-1.0	19234	188	Statut de minorité visible du répondant.

Tableau B.1 : Groupes et variables (suite)

Groupe Utilisation d'Internet, risques et prévention							
#	Nom	Libellé	Type	Format	Valide	Non-valide	Question
10	IRP_Q100	Au cours du dernier mois, avez-vous utilisé Internet?	discrète	numeric-1.0	19414	8	Au cours du dernier mois, avez-vous utilisé Internet?
11	IRP_Q115	Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?	discrète	numeric-1.0	14387	5035	Au cours du dernier mois, combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques? Était-ce :
12	IRP_Q130	Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?	discrète	numeric-1.0	14427	4995	Au cours du dernier mois, combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?
13	IRP_Q135	Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?	discrète	numeric-1.0	14423	4999	Au cours du dernier mois, combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?
14	IRP_Q140	Au cours des 12 derniers mois, avez-vous utilisé Internet?	discrète	numeric-1.0	4961	14461	Au cours des 12 derniers mois, avez-vous utilisé Internet?

Tableau B.1 : Groupes et variables (suite)

15	IRP_Q160	Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace ?	discrète	numeric-1.0	14930	4492	Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace?
16	IRP_Q170	Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?	discrète	numeric-1.0	15491	3931	Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?
Tentative d'hameçonnage, Infection et fraude bancaire							
17	IRP_Q243	Problèmes de sécurité. Reçu des courriels frauduleux	discrète	numeric-1.0	13601	5821	Avez-vous rencontré l'un des problèmes de sécurité suivants sur Internet? Reçu des courriels frauduleux, de quelqu'un qui se fait passer pour une organisation fiable et légitime, demandant des renseignements personnels.
18	IRP_Q270	Quelqu'un a-t-il utilisé votre carte de crédit ou de guichet à partir d'une source Internet	discrète	numeric-1.0	14874	4548	Au cours des 12 derniers mois, quelqu'un a-t-il utilisé votre carte de crédit ou de guichet (ou les détails de votre carte) à partir d'une source Internet pour effectuer des achats ou retirer des fonds de votre compte sans votre autorisation ?
19	IRP_Q300	Situations suivantes? Des sommes supplémentaires ont été tirées de votre compte sans votre autorisation	discrète	numeric-1.0	7815	11607	Au cours des 12 derniers mois, vous est-il arrivé une des situations suivantes? Des sommes supplémentaires ont été tirées de votre compte sans votre autorisation.

Tableau B.1 : Groupes et variables (suite et fin)

Groupe Victimisation sur Internet							
#	Nom	Libellé	Type	Format	Valide	Non-valide	Question
20	IRP_Q340	Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?	discrète	numeric-1.0	15290	4132	Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?
21	IRP_Q360	Pour protéger votre sécurité sur Internet : ... traitez-vous seulement avec des organisations bien connues?	discrète	numeric-1.0	15149	4273	Pour protéger votre sécurité sur Internet : ... traitez-vous en ligne seulement avec des organisations et des entreprises bien connues?
22	IRP_Q370	Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?	discrète	numeric-1.0	15331	4091	Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?
23	IRP_Q380	Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	discrète	numeric-1.0	13717	5705	Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?
24	IRP_Q385	Pour protéger votre sécurité sur Internet: ... supprimez-vous régulièrement les fichiers Internet temporaires?	discrète	numeric-1.0	15038	4384	Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les fichiers Internet temporaires et les témoins de connexion Internet « cookie»?
25	IRP_Q390_1	Pour protéger votre sécurité sur Internet : ... utilisez-vous un pare-feu?	discrète	numeric-1.0	15356	4066	Pour protéger votre sécurité sur Internet: ... utilisez-vous un pare-feu?

ANNEXE C : CODIFICATION DE VARIABLES DE L'ENQUÊTE ESG UTILISÉES DANS CETTE RECHERCHE

Tableau C.1 : Codification de la variable revenu.

Revenu personnel annuel du répondant (INCM)		
Ancienne Catégorie	Nouveau nom (INCM_C)	
	Nouvelle Catégorie	Libellé
1. Aucun revenu	0	Pauvre
2. Moins de 5000 $		
3. 5000 à 9999 $		
4. 10000 à 14999 $		
5. 15000 à 19999 $		
6. 20000 à 29999 $		
7. 30000 à 39999 $		
8. 40000 à 49999 $	1	Classe moyenne
9. 50000 à 59999 $		
10. 60000 à 79999 $		
11. 80000 à 99999 $	2	Riche
12. 100000 et plus		
MISSING VALUES	INCM_C (99.00, 98.00)	

Tableau C.2 : Utilisation d'Internet pour les opérations bancaires, les réservations et les achats

Combien de fois avez-vous utilisé Internet : ... pour effectuer les opérations bancaires électroniques, les réservations électroniques, les achats en ligne (IRP_Q115_C, IRP_Q130_C, IRP_Q135_C)		
Ancienne Catégorie	Nouveaux noms (IRP_Q130_C, IRP_Q135_C)	
	Nouvelle Catégorie	Libellé
1. …au moins une fois par jour	inchangé	inchangé
2. ….au moins une fois par semaine	inchangé	inchangé
3. ….au moins une fois par mois	inchangé	inchangé
4. ….pas au cours du dernier mois?	inchangé	inchangé
5. 6 ... jamais	5	5
7. Non demandé	inchangé	Missing
8. Non déclaré	inchangé	Missing
9. Ne sait pas	inchangé	Missing

Tableau C.3 : Contremesures de sécurité, à la victimisation et à l'utilisation d'Internet.

Ancienne Catégorie : IRP_Q160, IRP_Q170, IRP_Q243, IRP_Q340, IRP_Q360, IRP_Q370, IRP_Q380, IRP_Q385, IRP_Q390_1IRP_Q240	Nouveaux noms (IRP_Q160_C, IRP_Q170_C, IRP_Q243_C, IRP_Q340_C, IRP_Q360_C, IRP_Q370_C, IRP_Q380_C, IRP_Q385_C, IRP_Q390_1_C)	
	Nouvelle Catégorie	Libellé
1. Oui	inchangé	inchangé
2. Non	0	Non
7. Non demandé (7)	inchangé	Missing
8. Non déclaré (8)	inchangé	Missing
9. Ne sait pas (9)	inchangé	Missing

Tableau C.4 : Codification de la variable niveau de scolarité

Ancienne Catégorie : EDU10 -	Nouveaux noms (EDU_C)	
	Nouvelle Catégorie	Libellé
1. École primaire/aucune scolarité (10)	11	Niveau primaire
2. Études partielles au secondaire/l'école secondaire (9) 3. Diplôme d'études secondaires -DES- (8) 4. Études partielles à l'école de métiers/de formation technique (7) 5. Diplôme/d'études de l'école métiers/de formation technique(4)	12	Niveau secondaire
10. Collège communautaire/cégep/sciences infirmières (6) 11. Diplôme/certificat d'études d'un collège communautaire (3)	13	Niveau collégial
12. Études partielles à l'université (5) 13. Baccalauréat (2) 14. Doctorat/maîtrise/études partielles à l'université de troisième (1)	14	Niveau universitaire
7. Non déclaré (98)	inchangé	Missing
8. Ne sait pas (99)	inchangé	Missing

Tableau C.5 : Codification de la variable emploi

Ancienne Catégorie : ACMYR -	Nouveaux noms (ACMYR_C)	
	Nouvelle Catégorie	Libellé
6. Travailler à un emploi rémunéré ou à son propre compte (1) 7. Travaux ménagers (5)	1	Est occupé avec son emploi
9. Bénévolat ou aide fournie à des personnes autres que des enfants (9) 10. S'occuper des enfants (4)	2	Est occupé mais bénévolement
8. Être aux études (3) 9. Chercher un emploi rémunéré (2) 10. Autre (10)	3	Est aux études
15. Congé de maternité ou de paternité (7) 16. Maladie de longue durée (8) 17. À la retraite (6)	4	Est disponible (gère son temps)
11. Non déclaré (98)	inchangé	Missing
12. Ne sait pas (99)	inchangé	Missing

Tableau C.6 : Codification de la variable état Civil du répondant

Ancienne Catégorie : MARSTAT-	Nouveaux noms (MARSTAT_C)	
	Nouvelle Catégorie	Libellé
1. Marié (e)	1	Marié ou vivant en union libre
2. Vivre en union libre		
3. Veuf (ve)	3	Veuf, séparé ou divorcé
4. Séparé (e)		
5. Divorcé (e)		
6. Célibataire (jamais légalement marié(e))	inchangé	Célibataire (jamais légalement marié(e))
8. Non déclaré	inchangé	Missing
9. Ne sait pas	inchangé	Missing

ANNEXE D : CERTIFICAT DE CONFORMITÉ ÉTHIQUE

POLYTECHNIQUE MONTRÉAL
LE GÉNIE EN PREMIÈRE CLASSE

CERTIFICAT DE CONFORMITÉ ÉTHIQUE

Le 22 mars 2017

M. Jude Jacob Nsiempba
Mme Nathalie de Marcellis-Warin
Département de mathématiques et génie industriel
M. José Fernandez
Département de génie informatique et génie logiciel
Polytechnique Montréal

N/Réf : Dossier CÉR-1617-15

Madame, Messieurs,

J'ai le plaisir de vous informer que les membres du Comité d'éthique de la recherche avec des êtres humains (CÉR) ont procédé à l'évaluation en comité restreint du projet de recherche intitulé « *Hameçonnage bancaire: un cadre d'analyse des facteurs de risque et de prise de décision basé sur les coûts avantages des contremesures* ».

Les membres du CÉR ayant examiné votre projet en ont recommandé l'approbation sur la base des précisions que vous nous avez fait parvenir hier.

Veuillez noter que le présent certificat est valable pour une durée d'un an, soit du **22 mars 2017 au 21 mars 2018**, pour le projet tel que soumis au Comité d'éthique de la recherche avec des êtres humains.

Nous vous saurions gré de nous faire parvenir un bref **rapport annuel** (http://www.polymtl.ca/recherche/document/deonto.php) afin de renouveler votre certificat au moins un mois avant l'expiration du présent certificat. La secrétaire du Comité d'éthique de la recherche avec des sujets humains devra également être informée de toute modification qui pourrait être apportée ultérieurement au protocole expérimental, de même que de tout problème imprévu pouvant avoir une incidence sur la santé et la sécurité des personnes impliquées dans le projet de recherche (sujets, professionnels de recherche ou chercheurs).

Je vous souhaite bonne chance dans la poursuite de vos travaux,

Delphine Périé-Curnier, présidente
Comité d'éthique de la recherche avec des êtres humains

c.c.: Céline Roehrig (DRIAI), Danielle Bilodeau (BRCDT), Melissa Mirabella (Finances)

Comité d'éthique de la recherche avec des êtres humains
Pavillon principal
Téléphone : 514 340-4990
Télécopieur : 514 340-4992
Céline Roehrig
Secrétaire du Comité d'éthique de la recherche
Courriel : celine.roehrig@polymtl.ca

Campus de l'Université de Montréal
2900, boul. Édouard-Montpetit
2500, chemin de Polytechnique
Montréal (Québec) Canada H3T 1J4

Adresse postale
C.P. 6079, succ. Centre-Ville
Montréal (Québec) Canada H3C 3A7

ANNEXE E : QUESTIONNAIRE ENQUÊTE

Questions d'ordre général

1. De quel sexe êtes-vous? [ ] Homme [ ] Femme [ ] Je préfère ne pas répondre
2. À quel groupe d'âge appartenez-vous?
   18 à 24 ans [ ] 25 à 34 ans [ ] 35 à 44 ans [ ] 45 à 54 ans [ ] 55 à 64 ans [ ] Plus de 65 ans [ ]

3. Quelle fonction occupez-vous dans votre organisation/entreprise ?

4. Quel est votre champ d'expertise ?

5. Combien d'années d'expérience avez-vous,
   En sécurité informatique ? / Dans la lutte contre le phishing ?

/

6. Au cours des 12 derniers mois, avez-vous été confronté directement ou indirectement à des tentatives d'hameçonnage réussi ? Oui [ ] Non [ ] Si oui, donnez un bref détail ?

7. Au cours des 12 derniers mois, avez-vous été confronté directement ou indirectement à des infections par hameçonnage ? Oui [ ] Non [ ] Si oui, donnez un bref détail ?

8. Au cours des 12 derniers mois, avez-vous été confronté directement ou indirectement à la fraude bancaire par hameçonnage ? Oui [ ] Non [ ] Si oui, donnez un bref détail ?

9. Au cours des 60 derniers mois, avez-vous été confronté directement à une situation de prise de décision d'achat d'une contremesure ? Oui [ ] Non [ ] Si oui, donnez un bref détail ?

Partie A. Objectif : Identifier les facteurs probables qui influent sur le processus de monétisation[70] dans un marché noir.

Nous avons développé un modèle microéconomique pour analyser le marché noir des renseignements volés par hameçonnage. Cette analyse a permis d'identifier un certain nombre de variables probables qui influent sur le processus de monétisation. C'est pour avoir votre opinion d'expert sur ces éléments et leur degré d'influence que nous avons élaboré ces questions.

Facteurs qui influent sur le processus de monétisation

On vous demande de classer, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), l'influence de chacun de ces facteurs sur les chances de monétiser les renseignements bancaires volés par hameçonnage.						
1. Le revenu anticipé par le fraudeur / ce qu'il espère gagner	1	2	3	4	5	S/O
2. La probabilité de se faire arrêter et d'être sanctionné	1	2	3	4	5	S/O
3. L'investissement (la richesse ou le capital) initial du fraudeur pour acquérir les renseignements et autres ressources (ex. pour clonage) nécessaire au marché noir	1	2	3	4	5	S/O
4. Le montant de la commission payée aux tierces parties (ex. mule), le cas échéant.	1	2	3	4	5	S/O
5. La qualité des renseignements à monétiser (type de cartes, montant disponible, informations supplémentaires sur la victime, provenance de la carte –Amérique versus Europe, etc.)	1	2	3	4	5	S/O
6. Le temps écoulé entre le vol de renseignement et la fraude (retrait d'argent du compte de la victime)	1	2	3	4	5	S/O
7. Niveaux des mesures de sécurité opérationnelle mises en place par les banques	1	2	3	4	5	S/O
8. L'anonymat	1	2	3	4	5	S/O
9. Le prix de chaque renseignement au marché noir	1	2	3	4	5	S/O
Donner 3 autres facteurs qui, selon vous, contribuent à augmenter le risque de monétisation des renseignements personnels volés par hameçonnage? Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), l'influence de chacun de ces facteurs sur les chances de monétiser les renseignements bancaires volés par hameçonnage.						
10.	1	2	3	4	5	S/O
11.	1	2	3	4	5	S/O
12.	1	2	3	4	5	S/O

[70] C'est l'ensemble des actions qui concourent à soutirer l'argent d'un compte en utilisant des renseignements personnels dérobés auprès des victimes et vendus dans des forums clandestins.

Partie B. Objectif : Améliorer les contremesures au niveau de l'utilisateur et des organisations

L'examen des mesures de lutte contre l'hameçonnage bancaire a relevé un certain nombre d'insuffisances. Dans cette partie du questionnaire, nous voulons avoir votre avis d'expert sur ces insuffisances et les améliorations que vous suggérez pour les corriger. De la sorte, il sera possible d'examiner l'écart entre vos recommandations en tant qu'experts et l'état de la situation actuelle eu égard aux facteurs clés que nous avons déterminés grâce à notre cadre d'analyse.

Contremesures à améliorer

Filtres anti-hameçonnage	
On vous demande de classer par ordre d'efficacité les mesures de réduction des taux d'erreurs (faux positifs, faux négatifs) des filtres anti-hameçonnage ci-dessous sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet)	
- Meilleur réglage des critères de rejet (listes de restriction)	1 2 3 4 5 S/O
- Signature numérique	1 2 3 4 5 S/O
- Mécanismes d'empreinte avec authentification de l'émetteur	1 2 3 4 5 S/O
- Formation de base en sécurité	1 2 3 4 5 S/O
- Campagne de sensibilisation continue aux enjeux de sécurité (ex. menaces)	1 2 3 4 5 S/O
Donner 3 autres mesures qui, selon vous, contribuent à réduire le taux d'erreurs (faux positifs, faux négatifs) des filtres anti-hameçonnage? Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), le niveau d'efficacité de chacune de ces mesures.	
13.	1 2 3 4 5 S/O
14.	1 2 3 4 5 S/O
15.	1 2 3 4 5 S/O
Gestion des barres d'outils et des mots de passe	
On vous demande de classer par ordre d'efficacité à réduire le risque d'hameçonnage, les mesures de sécurisation des navigateurs et de gestion des mots de passe ci-dessous sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet)	
- Mise en place d'une barre d'outils standard pour les navigateurs dans toute l'organisation	1 2 3 4 5 S/O
- Mise en place d'un module standard de gestion des mots de passe Web pour toute l'organisation	1 2 3 4 5 S/O
- Adoption d'un navigateur standard pour toute l'organisation	1 2 3 4 5 S/O
- Systèmes d'alerte anti-phishing actifs (intégrés) dans les navigateurs	1 2 3 4 5 S/O
- Certificat EV SSL à validation étendue	1 2 3 4 5 S/O
- Authentification multifactorielle	1 2 3 4 5 S/O
Donner 3 autres mesures de sécurisation des navigateurs qui, selon vous, contribuent à réduire le risque d'hameçonnage? Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), le niveau d'efficacité de chacune de ces mesures.	
16.	1 2 3 4 5 S/O
17.	1 2 3 4 5 S/O
18.	1 2 3 4 5 S/O
Listes de restriction et fichiers de journalisation Sur une échelle de 1 à 5 (1 pour Très insatisfait, 2 pour Plutôt insatisfait, 3 pour Neutre, 4 pour Plutôt satisfait et 5 pour Très satisfait, S/O= Sans objet)	
Quel est votre degré de satisfaction à l'égard du temps moyen de mise à jour des listes de restrictions (liste noire) dans votre organisation.	1 2 3 4 5 S/O

Quel est votre degré de satisfaction à l'égard du temps moyen de mise à jour des listes de restrictions/fichiers de journalisation pour des sites de phishing hébergés au Canada	1 2 3 4 5 S/O
Quel est votre degré de satisfaction à l'égard du temps moyen de mise à jour des listes de restrictions/fichiers de journalisation pour des sites de phishing hébergés à l'étranger	1 2 3 4 5 S/O
Dans l'ensemble, quel est votre degré de satisfaction à l'égard de la collaboration entre les partenaires (force de police et organismes anti-phishing)	1 2 3 4 5 S/O
Dans l'ensemble, quel est votre degré de satisfaction à l'égard de la collaboration entre pays dans la lutte anti-phishing ?	1 2 3 4 5 S/O
Que pensez-vous des solutions juridiques visant à favoriser l'échange des listes noires entre partenaire dans la lutte contre le phishing et sur les questions entourant les faux positifs de listes noires ? (1 pour Tout à fait en désaccord, 2 pour Plutôt en désaccord, 3 pour Neutre, 4 pour Plutôt en accord et 5 pour Tout à fait en accord, S/O= Sans objet)	1 2 3 4 5 S/O
Comment peut-on améliorer la mise à jour des listes de restrictions et des fichiers de journalisation? On vous demande de faire 3 suggestions de mesures à prendre pour améliorer la mise à jour des listes de restriction et des fichiers de journalisation. Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), le niveau d'efficacité de chacune de ces mesures.	
19.	1 2 3 4 5 S/O
20.	1 2 3 4 5 S/O
21.	1 2 3 4 5 S/O
Sécurisation de l'information lors les transactions bancaires en ligne On vous demande de classer par ordre d'efficacité à réduire le risque de fraude, les mesures de sécurisation des transactions bancaires ci-dessous sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet)	
- Chiffrement des transactions	1 2 3 4 5 S/O
- Témoins[71]	1 2 3 4 5 S/O
- Authentification de transaction en ligne par des protocoles suivants : - 3D-Secure ou Verified By Visa et MasterCard SecureCode,	1 2 3 4 5 S/O
- Authentification biométrique - Signature électronique	1 2 3 4 5 S/O
Donner 3 autres mesures de sécurisation des renseignements bancaires à mettre en place pour réduire le risque de fraude en ligne? Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), le niveau d'efficacité de chacune de ces mesures.	
22.	
23.	
24.	
Formations et campagnes de sensibilisation sur les enjeux de sécurité	

[71] C'est un fichier contenant des éléments d'information que le site Web de la banque crée automatiquement lorsqu'un client le visite. Par exemple, lorsqu'un client se connecte à «service Net» d'une banque, le serveur du «service Net» capture ces informations et pendant toute la durée de la session d'utilisation, il fait les vérifications nécessaires pour s'assurer que la banque fait affaire avec le bon client.

Sur une échelle de 1 à 5 (1 pour Très insatisfait, 2 pour Plutôt insatisfait, 3 pour Neutre, 4 pour Plutôt satisfait et 5 pour Très satisfait, S/O= Sans objet)	
Quel est votre degré de satisfaction à l'égard de la formation anti-phishing individuelle pour reconnaître les sites usurpés, les faux noms de domaine, les hyperliens truqués, les différents stratagèmes, etc. dans votre organisation	1 2 3 4 5 S/O
Quel est votre degré de satisfaction à l'égard de la formation anti-phishing de groupe (ex. dispensée par l'entreprise sur le lieu de travail et avec le matériel de travail).	1 2 3 4 5 S/O
Quel est votre degré de satisfaction à l'égard des campagnes grand-public utilisant les réseaux sociaux pour sensibiliser le public sur le phishing, le cybermarché et ses acteurs (ex. les mules)	1 2 3 4 5 S/O
Quel est votre degré de satisfaction à l'égard des développements des outils de formation (ex. en utilisant les micro-jeux)	1 2 3 4 5 S/O
Comment peut-on améliorer les formations et les campagnes de sensibilisation aux enjeux de sécurité? On vous demande de faire 3 suggestions de mesures à prendre pour améliorer la formation et la sensibilisation du public aux enjeux de sécurité. Classez, sur une échelle de 1 à 5 (1 pour très faible, 2 pour faible, 3 pour moyenne, 4 pour forte et 5 pour très forte, S/O= Sans objet), le niveau d'efficacité de chacune de ces mesures.	
25.	1 2 3 4 5 S/O
26.	1 2 3 4 5 S/O
27.	1 2 3 4 5 S/O

Partie C : prise de décision dans le choix des contremesures

Objectif : Comment choisir la contremesure avec le meilleur rapport "mitigation de risque" versus "Coût en prévention" induit par l'acquisition celle-ci ?

On vous demande de classer, sur une échelle de 1 à 5 (1 pour Pas du tout important, 2 pour Peu important, 3 pour Légèrement important, 4 pour Très important et 5 pour Extrêmement important, S/O= Sans objet), les critères de décision que vous favorisez pour l'acquisition d'une contremesure de sécurité ?	
- La mitigation de risque	1 2 3 4 5 S/O
- Le revenu induit[72] par l'acquisition de la contremesure	1 2 3 4 5 S/O
- Les coûts en prévention[73] engendré par l'acquisition de la contremesure	1 2 3 4 5 S/O
- Réputation /popularité du fabricant (part de marché)	1 2 3 4 5 S/O
- Interopérabilité /compatibilité avec les systèmes et applications en place	1 2 3 4 5 S/O
Donner 3 autres critères (spécifiez)	
28.	1 2 3 4 5 S/O
29.	1 2 3 4 5 S/O
30.	1 2 3 4 5 S/O

Entretien non directif pour la question du suit.

Dans votre organisation, comment mesurez-vous (métrique utilisées) le retour sur investissement (ROI) d'une contremesure de sécurité ?

[72] À titre d'exemple, on peut invoquer l'économie réalisée en termes de réduction des frais de réparation ou de réduction des primes d'assurance du fait de l'acquisition et de l'utilisation d'une contremesure.

[73] Il s'agit des coûts d'investissement (logiciels, matériels) et des coûts des opérations (salaire, licence, formation, assurance, audits, perturbations causées par la mise en place de la contremesure, etc.)

ANNEXE F : COÛTS ASSOCIÉS AU RISQUE DE SÉCURITÉ INFORMATIQUE

Tableau F.1 : Catégories de coûts et exemples

Catégorie des coûts	**Sous-catégories**		**Exemples**
Coûts en prévention (CP)	Investissement (CPI)	Directs	- logiciel et matériel (ex. Antivirus, pare-feu, etc.)
		Indirects	- Serveurs, Switch
	Opérations (CPO)	Éléments tangibles	- Salaire suppl., - Impacts des perturbations causées par les contremesures
		Éléments intangibles	- Licences, mise à jour, - Formation, - Assurance, - Audits, conformité - Impacts des perturbations causées par les contremesures
Coûts en conséquence (CC)	Pertes directes (CCD)		- Perte de clients, - Pénalités et retard - Juridiques, - Honoraires experts, - Remplacement.
	Coûts indirects (CCI)		- Compétitivité affaiblie en tant que résultat d'un compromis de propriété intellectuelle
Coûts en réponse (CP)	Coûts essentiellement directs		- Indemnités (versées aux victimes), amendes (versées aux organismes de règlementation, etc.)
Autres coûts difficilement mesurables (CDQ)	Coûts indirects		- Image, réputation - Économie souterraine - Courbe d'apprentissage - Impact sur les partenaires - Nouveaux clients

ANNEXE G : FACTEURS DE RISQUE INDIVIDUELS -TABLEAUX CROISÉS-

Tableau G.1 : Corrélations entre la victimisation et les caractéristiques sociodémographiques

		Tentative d'hameçonnage		Infection		Fraude	
		(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»
SEX : Genre	F	33%	36,00%	60%	56,30%	4%	4,00%
	M	45%	49,00%	70%	66,70%	4%	3,90%
	Rés. global	**39%**	**42,00%**	**65%**	**61,10%**	**4%**	**4,00%**
AGEGR10 : Groupes d'âge du répondant	15 à 24	35%	34,40%	69%	67,90%	3%[E]	3,40%
	25 à 34	43%	45,40%	70%	68,40%	4%	4,10%
	35 à 44	44%	47,40%	68%	66,10%	5%*	4,30%
	45 à 54	39%	43,60%	67%	63,00%	4%*	4,30%
	55 à 64	37%	40,80%	59%	54,70%	4%*	3,30%
	65 à 74	29%	35,10%	43%	44,00%	3%[E]	4,40%
	75 ans et +		29,10%		31,30%		2,00%
	Rés. global		**42,00%**		**61,10%**		**4,00%**
MARSTAT : État matrimonial	Marié(e)		43,70%		61,40%	4%	3,90%
	Vivant en union libre		39,80%		63,20%	4%	3,40%
	Veuf (ve)		30,70%		36,80%	F	1,40%
	Séparé(e)		42,10%		62,50%	3%	6,40%
	Divorcé(e)		44,40%		57,40%	3%	6,70%
	Rés. global		42,4%		59,90%		4,1%
EDU10 : Niveau de scolarité	Université	54%	52,90%	70%	67,40%	5%	3,90%
	Collégial	37%	47,70%	65%	61,30%	4%	4,10%
	Secondaire (diplômé)	25%	43,70%	57%	52,10%	3%	3,10%
	Primaire	21%	37,90%	59%	52,00%	1%	3,00%
	Rés. global		**44,00%**		**61,00%**	**5%**	**4,00%**
LANHSDC : Langue	Anglais	43%	44,80%	65%	60,70%	4%	4,00%
	Français	25%	29,40%	65%	61,90%	3%	3,20%
	Autres	36%	41,50%	63%	63,70%	5%	4,70%
	Rés. global		**42,00%**		**61,10%**		**4,00%**
LUC_RST : Indicateur urbain/rurale	RMR	43%	44,10%	67%	62,90%	4%	4,00%
	Hors RMR	30%	33,60%	60%	55,00%	2%	1,9%
	Île-du-Prince-Édouard		41,20%		54,00%		1,70%

[E] à utiliser avec prudence

* Différence significative par rapport à la catégorie de référence ($p < 0,05$)

[F] Trop peu fiable pour être publié

Tableau G.2 : Corrélations entre la victimisation et les caractéristiques économiques

		Tentative d'hameçonnage		Infection		Fraude	
		(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»
INCM: …Revenu personnel annuel	20K et moins	33%	34,20%	65%	60,26%	2%	3,70%
	20K à 39,9K	34%	36,40%	62%	56,85%	3%	4,15%
	40K à 59,9K	38%	42,90%	64%	60,75%	4%	3,50%
	60K à 99,9K	50%	54,45%	71%	69,05%	6%	3,35%
	100K ou+	58%	60,10%	76%	72,60%	6%	4,50%
ACMYR : Activité principale	Emploi rémunéré ou à son compte		45,40%		63,70%		3,90%
	Chercher un emploi rémunéré		44,70%		67,80%		4,20%
	Être aux études		35,60%		69,10%		4,00%
	S'occuper des enfants		37,10%		62,30%		3,90%
	Travaux ménagers		32,40%		52,10%		3,40%
	À la retraite		34,10%		45,70%		3,90%
	Congé de maternité /paternité		43,50%		68,80%		7,90%
	Maladie de longue durée		40,90%		55,40%		8,20%
	Bénévolat ou aide fournie à des personnes autres que des enfants		36,00%		48,50%		0,00%
	Autre		33,30%		52,60%		5,00%

Tableau G.3 : Corrélations entre la victimisation et les origines des victimes

		Tentative d'hameçonnage		Infection		Fraude	
		(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»
BPR_Q50 : Immigrant reçu	oui	38%	45,80%	65%	61,40%	4%	5,80%
	non	42%	50,60%	64%	61,90%	4%	4,10%
	Rés. global		46,40%		61,50%		5,60%
VISMIN : Minorité visible	oui	39%	44,00%	65%	65,10%	4%	7,00%
	non	42%	41,70%	67%	60,70%	4%	3,70%
	Rés. global		42,00%		61,10%		4,00%
AIR_Q110 : Autochtone	Oui		37,20%		56,50%		5,50%
	Non		42,20%		61,30%		3,90%
	Rés. global		42,00%		61,10%		4%

Tableau G.4 : Corrélations entre la victimisation et les comportementales en ligne

		Tentative d'hameçonnage		Infection		Fraude	
		(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»
IRP_Q130 :…Réservations en ligne	Au moins une fois par jour		57,50%		70,70%		5,70%
	Au moins une fois par semaine	64%	64,50%	78%	76,80%	8%	5,60%
	Au moins une fois par mois	54%	55,70%	71%	69,80%	6%	4,30%
	Occasionnellement	42%	44,20%	68%	65,50%	3%	3,70%
	Rarement ou jamais	26%	29,40%	59%	55,80%	3%	3,20%
	Rés. global		42,40%		63,10%		3,90%
IRP_Q115 : …opérations bancaires en ligne	Au moins une fois par jour		53,40%		69,00%	5%	5,40%
	Au moins une fois par semaine	50%	49,50%	69%	67,10%	5%	4,20%
	Au moins une fois par mois	43%	45,90%	70%	67,50%	4%	3,90%
	Occasionnellement	32%	34,40%	65%	62,10%	4%	2,50%
	Rarement ou jamais	25%	29,50%	58%	54,80%	2%	2,60%
	Rés. global		42,40%		63,20%		3,90%
IRP_Q135 : …..Achats en ligne	Au moins une fois par jour		62,80%		72,70%	7%	6,70%
	Au moins une fois par semaine	66%	65,50%	74%	73,20%	7%	4,40%
	Au moins une fois par mois	56%	56,70%	73%	71,30%	5%	4,30%
	Occasionnellement	41%	44,20%	68%	66,20%	4%	3,30%
	Rarement ou jamais	24%	27,20%	58%	54,00%	3%	3,30%
	Rés. global		42,40%		63,10%		3,90%
IRP_Q170 : Utilisation des réseaux sociaux en ligne	oui	45%	47,00%	71%	68,70%	4%	4,80%
	non	32%	37,10%	59%	56,80%	4%	2,90%
	Rés. global		42,00%		62,30%		4,00%
IRP_Q160 : Utilisation des salons de clavardage en ligne	oui	48%	50,40%	76%	75,00%	3%	4,80%
	non	35%	38,50%	60%	56,00%	4%	3,50%
	Rés. global		42,00%		61,00%		4,00%

Tableau G.5 : Corrélations entre la victimisation et les contremesures de sécurité

		Tentative d'hameçonnage		Infection		Fraude	
		(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»	(Perreault, 2013)	«notre étude»
IRP_Q360 : Transactions effectuées seulement avec des organisations biens connues	oui	41%	43,10%	66%	62,80%	4%	3,80%
	non	32%	37,80%	61%	54,00%	3%	5,10%
	Rés. global		42,40%		61,50%		4,00%
IRP_Q380 : supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	oui	43%	43,40%	68%	65,20%	4%	4,00%
	non	29%	27,00%	60%	53,90%	3%	3,70%
	Rés. global		42,10%		64,30%		4,00%
IRP_Q385 : Supprimer régulièrement les fichiers temporaires	oui	43%	43,40%	44,80%	69%		4%
	non	29%	27,00%	34,20%	55%		3%
	Rés. global		42,40%		61,60%		4,00%
IRP_Q370 : changez-vous régulièrement vos mots de passe?	oui	44%	46,90%	67%	64,00%	4%	3,80%
	non	37%	39,40%	64%	59,90%	4%	4,00%
	Rés. global		42,00%		61,30%		3,90%
IRP_Q340 : Utiliser un logiciel antivirus	oui	40%	42,60%	67%	64,20%	4%	3,90%
	non	38%	38,40%	45%	23,60%	4%	4,90%
	pas d'ordinateur		23,20%				
	Rés. global		**42,20%**		**61,40%**		**4,00%**
IRP_Q390_1 : Utiliser un pare-feu*	oui	?	73,00%	?	79,40%	?	4,60%
	non	?	41,50%	?	61,00%	?	3,90%
	Rés. global		**42,00%**		**61,30%**		**4,00%**

Tableau G.6 : Classement des facteurs de risque de tentative d'hameçonnage

			Proportion
IRP_Q135 : …..Achats en ligne	Rarement ou jamais	Au moins une fois par jour	2
IRP_Q115 : …opérations bancaires en ligne	Rarement ou jamais	Au moins une fois par jour	2
IRP_Q130 :…Réservations en ligne	Rarement ou jamais	Au moins une fois par jour	1,8
INCM: …Revenu personnel annuel	20K et moins	100K et +	1,75
IRP_Q390_1 : Utiliser un pare-feu*	Oui	Non	1,75
LANHSDC : Langue	Francophone	Anglophone	1,72
ACMYR : Activité principale	Travaux ménagers	Emploi rémunéré ou à son compte	1,40
SEX : Genre	Femme	Homme	1,36
LUC_RST : Indicateur urbain/rurale	Hors RMR	RMR	1,31
EDU10 : Niveau de scolarité	Primaire	Collège /Université	1,3
IRP_Q160 : Utilisation des salons de clavardage en ligne	Non	oui	1,30
IRP_Q170 : Utilisation des réseaux sociaux en ligne	Non	oui	1,26
IRP_Q340 : Utiliser un logiciel antivirus	Non	Oui	0,90**
IRP_Q360 : Transactions effectuées seulement avec des organisations biens connues	Non	Oui	0,87**
IRP_Q370 : changez-vous régulièrement vos mots de passe?	Non	Oui	0,84**
IRP_Q380 : supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	Non	Oui	0,62**
IRP_Q385 : Supprimer régulièrement les fichiers temporaires	Non	Oui	0,62**

* facteur non étudié dans les travaux antérieurs

**les internautes qui n'ont pas pris cette contremesure ont déclaré avoir été moins victimes de tentative d'hameçonnage. La contre mesure semble avoir contribué à augmenter le risque d'hameçonnage réussie.

Tableau G.7 : Classement des facteurs de risque d'infection

			Proportion
IRP_Q160 : Utilisation des salons de clavardage en ligne	Non	oui	1,33
ACMYR : Activité principale	Travaux ménagers (52,10%)	Être aux études (69,10%)	1,32
IRP_Q130 :…Réservations en ligne	Rarement ou jamais	Au moins une fois par jour	1,3
IRP_Q135 : …..Achats en ligne	Rarement ou jamais	Au moins une fois par jour	1,3
IRP_Q115 :…opérations bancaires en ligne	Rarement ou jamais	Au moins une fois par jour	1,3
IRP_Q390_1 : Utiliser un pare-feu*	Non	Non	1,3
EDU10 : Niveau de scolarité	Primaire	Collège /Université	1,3
INCM: …Revenu personnel annuel	20K à 39,9K (56,85%)	100K et + (72,60%)	1,27
IRP_Q170 : Utilisation des réseaux sociaux en ligne	Non	oui	1,20
SEX : Genre	Femme	Homme	1,18
LUC_RST : Indicateur urbain/rurale	Hors RMR (55%)	RMR (62,9%)	1,14
IRP_Q370 : changez-vous régulièrement vos mots de passe?	Non	Oui	0,935**
IRP_Q360 : Transactions effectuées seulement avec des organisations biens connues	Non	Oui	0,859**
IRP_Q380 : supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	Non	Oui	0,826**
IRP_Q385 : Supprimer régulièrement les fichiers temporaires	Non	Oui	0,797**
IRP_Q340 : Utiliser un logiciel antivirus	Non	Oui	0,37**

* facteur non étudié dans les travaux antérieurs

**les internautes qui n'ont pas pris cette contremesure ont déclaré avoir été moins victimes d'infection. La contre mesure semble avoir contribué à augmenter le risque d'infection.

Tableau G.8 : Classement des facteurs de risque de fraude

			Proportion
ACMYR: Activité principale	Travaux ménagers	Maladie de longue durée/ Congé de maternité /paternité	2,41
LUC_RST : Indicateur urbain/rurale	Hors RMR (1,9%)	RMR (4%)	2,1
IRP_Q135 :…..Achats en ligne	Rarement ou jamais	Au moins une fois par jour	2
IRP_Q115 :…opérations bancaires en ligne	Rarement ou jamais	Au moins une fois par jour	2
VISMIN : Minorité visible	Non	Oui	1,9
IRP_Q130 :…Réservations en ligne	Rarement ou jamais	Au moins une fois par jour	1,8
MARSTAT : État matrimonial	Divorcé/séparé	Marié/union libre	1,6-2
IRP_Q170 : Utilisation des réseaux sociaux en ligne	Non	Oui	1,65
AIR_Q110 : Autochtone	Non	Oui	1,41
BPR_Q50 : Immigrant reçu	Non	Oui	1,4
IRP_Q160 : Utilisation des salons de clavardage en ligne	Non	Oui	1,37
INCM:…Revenu personnel annuel	60K à 99,9K (3,35%)	100K et + (4,50%)	1,34
EDU10 : Niveau de scolarité	Primaire	Collège /Université	1,3
LANHSDC : Langue	Francophone	Anglophone	1,25
IRP_Q340 : Utiliser un logiciel antivirus	Non	Oui	1,25
IRP_Q390_1 : Utiliser un pare-feu*	Non	Oui	1,15
SEX : Genre	Femme	Homme	1,1
IRP_Q370 : changez-vous régulièrement vos mots de passe?	Non	Oui	1,1
IRP_Q385 : Supprimer régulièrement les fichiers temporaires	Non	Oui	1,05
IRP_Q360 : Transactions effectuées seulement avec des organisations biens connues	Non	Oui	.925**
IRP_Q380 : Supprimer régulièrement les courriels envoyés par des expéditeurs inconnus	Non	Oui	0,75**

* facteur non étudié dans les travaux antérieurs

**les internautes qui n'ont pas pris cette contremesure ont déclaré avoir été moins victimes de fraude. La contre mesure semble avoir contribué à augmenter le risque d'infection !!

ANNEXE H : FACTEURS DE RISQUE-RÉGRESSION LOGISTIQUE

Tableau H.1 : Accroissement du risque de tentative d'hameçonnage

Variables et description	B	Sig.	Exp(B)
IRP_Q390_1 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un pare-feu?	,834	,000	2,302
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?		,000	
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(1)	,375	,000	1,454
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(2)	,304	,000	1,356
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(3)	,298	,000	1,348
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(4)	-,075	,425	,928
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?		,000	
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(1)	,390	,313	1,477
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(2)	,377	,003	1,458
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(3)	,354	,000	1,425
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(4)	,133	,021	1,142
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?		,000	
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(1)	,892	,020	2,440
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(2)	,846	,000	2,330
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(3)	,596	,000	1,814
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(4)	,317	,000	1,373
IRP_Q160 codifié : Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace?	,242	,000	1,274
IRP_Q170 codifié : Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?	,447	,000	1,564
IRP_Q370 codifié : Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?	,129	,004	1,138
IRP_Q380 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	,346	,000	1,413
IRP_Q385 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les fichiers Internet temporaires?	,169	,002	1,184
Sexe du répondant.(1)	,502	,000	1,653
Langue du ménage du répondant.		,000	

Tableau H.1 : Accroissement du risque de tentative d'hameçonnage (suite et fin)

Langue du ménage du répondant.(1)	,271	,002	1,311
Langue du ménage du répondant.(2)	-,464	,000	,629
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.		,000	
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(1)	,000	,999	1,000
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(2)	-,668	,000	,513
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(3)	-,473	,000	,623
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois		,211	
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(1)	,025	,697	1,026
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(2)	,026	,813	1,026
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(3)	-,125	,158	,883
IRP_Q340 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?	,170	,071	1,185
IRP_Q360 codifié : Pour protéger votre sécurité sur Internet : ... traitez-vous seulement avec des organisations bien connues?	-,029	,661	,971
INCM codifié : Revenu personnel annuel du répondant		,000	
INCM codifié : Revenu personnel annuel du répondant(1)	-,336	,000	,715
INCM codifié : Revenu personnel annuel du répondant(2)	-,240	,000	,787
Indicateur urbain/rurale.(1)	,239	,000	1,270
Constante	-1,813	,000	,163

Tableau H.2 : Accroissement du risque d'infection

Variables et description	B	Sig.	Exp(B)
IRP_Q390_1 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un pare-feu?	,216	,226	1,241
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?		,106	
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(1)	,062	,435	1,064
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(2)	,051	,369	1,053
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(3)	,176	,009	1,192
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(4)	-,001	,991	,999
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?		,102	
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(1)	,391	,355	1,478
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(2)	,317	,021	1,373
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(3)	,126	,049	1,135
IRP_Q130 codifié +: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(4)	,087	,131	1,091

Tableau H.2 : Accroissement du risque d'infection (suite et fin)

IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?		,000	
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(1)	,321	,426	1,379
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(2)	,221	,055	1,247
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(3)	,293	,000	1,341
IRP_Q135 codifié +: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(4)	,218	,000	1,243
IRP_Q160 codifié : Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace?	,173	,000	1,188
IRP_Q170 codifié : Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?	,562	,000	1,755
IRP_Q370 codifié : Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?	-,039	,391	,962
IRP_Q380 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	,199	,014	1,220
IRP_Q385 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les fichiers Internet temporaires?	,213	,000	1,238
Sexe du répondant.(1)	,526	,000	1,692
Langue du ménage du répondant.		,392	
Langue du ménage du répondant.(1)	,094	,281	1,099
Langue du ménage du répondant.(2)	,134	,171	1,144
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.		,000	
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(1)	-,703	,021	,495
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(2)	-,272	,000	,762
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(3)	-,122	,032	,885
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois		,000	
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(1)	,393	,000	1,482
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(2)	,518	,000	1,678
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(3)	,541	,000	1,718
IRP_Q340 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?	,927	,000	2,528
IRP_Q360 codifié : Pour protéger votre sécurité sur Internet : ... traitez-vous seulement avec des organisations bien connues?	,004	,947	1,004
INCM codifié : Revenu personnel annuel du répondant		,117	
INCM codifié : Revenu personnel annuel du répondant(1)	-,132	,079	,876
INCM codifié : Revenu personnel annuel du répondant(2)	-,141	,042	,869
Indicateur urbain/rurale. (1)	,155	,003	1,167
Constante	-1,633	,000	,195

Tableau H.3 : Accroissement du risque de fraude

Variables et description	B	Sig.	Exp(B)
IRP_Q390_1 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un pare-feu?	,227	,461	1,255
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?		,050	
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(1)	,562	,003	1,755
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(2)	,276	,077	1,317
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(3)	,352	,048	1,421
IRP_Q115 codifié +: Combien de fois avez-vous utilisé Internet : ... pour effectuer des opérations bancaires électroniques?(4)	,207	,418	1,230
IRP_Q130 codifié: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?		,243	
IRP_Q130 codifié: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(1)	-,664	,525	,515
IRP_Q130 codifié: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(2)	,231	,342	1,260
IRP_Q130 codifié: Combien de fois avez-vous utilisé Internet : ... pour faire une réservation en ligne?(3)	,220	,066	1,247
IRP_Q135 codifié: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?		,045	
IRP_Q135 codifié: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(1)	,927	,142	2,526
IRP_Q135 codifié: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(2)	,350	,109	1,418
IRP_Q135 codifié: Combien de fois avez-vous utilisé Internet : ... pour acheter des produits ou des services?(3)	,286	,016	1,331
IRP_Q160 codifié : Appartenez-vous à un groupe de réseautage social en ligne comme Facebook ou MySpace?	,036	,756	1,036
IRP_Q170 codifié : Avez-vous déjà utilisé Internet pour vous connecter à un service de clavardage en ligne?	,041	,737	1,042
IRP_Q370 codifié : Pour protéger votre sécurité sur Internet : ... changez-vous régulièrement vos mots de passe?	-,103	,356	,902
IRP_Q380 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les courriels d'expéditeurs inconnus?	,203	,387	1,225
IRP_Q385 codifié : Pour protéger votre sécurité sur Internet : ... supprimez-vous régulièrement les fichiers Internet temporaires?	-,054	,685	,948
Sexe du répondant.(1)	-,017	,879	,983
Langue du ménage du répondant.		,380	
Langue du ménage du répondant.(1)	-,156	,443	,855
Langue du ménage du répondant.(2)	-,315	,184	,730
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.		,136	
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(1)	-17,277	,998	,000
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(2)	-,065	,629	,937
EDU10 codifié : Le niveau de scolarité le plus élevé atteint par le répondant.(3)	,243	,060	1,275

Tableau H.3 : Accroissement du risque de fraude (suite et fin)

ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois		,349	
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(1)	,066	,704	1,068
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(2)	,322	,244	1,380
ACMYR codifié : Activité principale du répondant au cours des 12 derniers mois(3)	-,205	,432	,815
IRP_Q340 codifié : Pour protéger votre sécurité sur Internet : ... utilisez-vous un logiciel antivirus?	-,177	,418	,838
IRP_Q360 codifié : Pour protéger votre sécurité sur Internet : ... traitez-vous seulement avec des organisations bien connues?	,193	,282	1,213
INCM codifié : Revenu personnel annuel du répondant		,000	
INCM codifié : Revenu personnel annuel du répondant(1)	-,655	,000	,519
INCM codifié : Revenu personnel annuel du répondant(2)	-,152	,277	,859
Indicateur urbain/rurale.(1)	,256	,085	1,291
Constante	-3,701	,000	,025

Tableau H.4 : Liens entre les comportements à risque et le nombre de contremesures

	AV[74]	PF[75]	AV&PF	SME[76]	AV&PF &SME	CRM[77]	AV&PF& SME&CRM	SFT[78]	AV&PF&SME &CRM&SFT
	13239	252	237(1,2%)	12346	226 (1,2%)	4827	103 (0,5%)	10595	95 (0,5%)
Ont effectué des OBE[79]	8313 (62,8%) Khi-2(226,799; p=0.000)	195 (78,6%) Khi-2(34,465; p=0.000)	184 (77,65%) Khi-2(28,127; p=0.000)	8 071 (65,4%) Khi-2(130,645; p=0.000)	181 (80,1%) Khi-2(35690; p=0.000)	3260 (67,6%) Khi-2(131,640; p=0.000)	80 (77,7%) Khi-2(16845; p=0.002)	6995 (66%) Khi-2(301,114; p=0.002)	76 (80%) Khi-2(19708; p=0.001)
N'ont pas effectué des OBE	4926 (37,2%)	53 (21,4%)	53(22,36%)	4275 (34,6%)	45(19,9%)	1567 (32,4%)	23(22,3%)	3600 (44%)	19 (20%)
Ont acheter des produits et services	4053 (30,5%) Khi-2(126,345; p=0.000)	122 (49,2%) Khi-2(64,687; p=0.000)	113(47,6%) Khi-2(54,416; p=0.000)	4001 (32,3%) Khi-2(142,227; p=0.000)	109(48,3%) Khi-2(55579; p=0.000)	1631 (33,6%) Khi-2(59717; p=0.000)	48(46,7%) Khi-2(28,921; p=0.000)	3479 (32,7%) Khi-2(177,262; p=0.000)	47(49,5%) Khi-2(31,411; p=0.000)
N'ont pas acheter les produits et services	9221 (69,5%)	126 (50,8%)	124(52,3%)	8377 (67,7%)	117(51,8%)	3220 (66,4%)	55(53,4%)	7142 (67,3%)	48(40,5%)

[74] Ont déclaré avoir un antivirus seulement (IRP_Q340)

[75] Ont déclaré avoir un pare-feu seulement(IRP_Q390_1)

[76] Ont déclaré supprimer les mails d'expéditeurs inconnus seulement (var : IRP_Q8380)

[77] Ont déclaré changer les mots de passe seulement (var : IRP_Q370)

[78] Ont déclaré supprimer les fichiers temporaires (IRP_Q385)

[79] Opération bancaire électronique

Tableau H.4 : Liens entre les comportements à risque et le nombre de contremesures (suite et fin)

Ont fait une réservation en ligne	3689(27,8%) Khi-2(127,384; p=000)	107 (43,1%) Khi-2(41,663; p=0.000)	101(42,6%) Khi-2(37785; p=0.000)	3607 (29,2%) Khi-2(145,680; p=0.000)	97 (42,9%) Khi-2(37883; p=0.000)	1491 (30,7%) Khi-2(60,488; p=0.000)	50 (48,5%) Khi-2(27783; p=0.000)	3116 (29,3%) Khi-2(149,770; p=0.000)	47 (49,5%) Khi-2(28633; p=0.000)
N'ont pas fait une réservation en ligne	9587 (72,2%)	141 (56,9%)	136 (57,4%)	8777 (70,8%)	129 (57,1%)	3362 (69,3%)	53 (51,5%)	7509 (70,7%)	48 (50,5%)
Appartiennent à un réseau social	6460 (47,4%) Khi-2(106,840; p=0.000)	126 (50%) Khi-2(1,192; p=0.275)	118 (49%) ***	6331 (50,3%) Khi-2(27,627; p=0.000)	112 (48,9%)	2610 (52,3%) Khi-2(96,522; p=0.000)	47 (45,2%)	5489 (50,5%) Khi-2(200,167; p=0.000)	44 (45,8%)
N'appartiennent pas à un réseau social	7155 (52,6%)	126 (50%)	123 (51%)	6249 (49,7%)	117 (51,1%)	2378 (47,7%)	57 (54,8%)	5372 (49,5%)	52 (54,2%)
Utilisent un serv. de clavardage	3793 (27,4%) Khi-2(68,395; p=0.000)	124 (49,4%) Khi-2(67,476; p=0.000)	118 (49,2%) Khi-2(63111; p=0.000)	3665 (29,1%) Khi-2(,658; p=0.417)	113 (49,6%) Khi-2(62874; p=0.000)	1515 (29,6%) Khi-2(32,265; p=0.000)	53 (51,5%) Khi-2(32991; p=0.000)	3264 (29,6%) Khi-2(136,428; p=0.000)	48 (50,5%) Khi-2(28179; p=0.000)
N'utilisent pas un serv. de clavardage	10058 (72,6%)	127 (50,6%)	122 (50,8%)	8915 (70,1%)	115 (50,4%)	3601 (70,4%)	50 (48,5%)	7749 (70,4%)	47 (48,5%)

Tableau H.5 : Liens entre la victimisation et le nombre de contremesures

	AV[80]	PF[81]	AV&PF	SME[82]	AV&PF &SME	CRM[83]	AV&PF& SME&CRM	SFT[84]	AV&PF&SME &CRM&SFT
	13239	252	237(1,2%)	12346	226 (1,2%)	4827	103 (0,5%)	10595	95 (0,5%)
Tentative d'hameçonnage	5383(42,6%) Khi-2(19781; p=0.000)	178 (73%) Khi-2(97,563; p=0.000)	168 (72,1%) Khi-2(88,066; p=0.000)	5406 (43,4%) Khi-2(112,957; p=0.000)	163 (72,4%) Khi-2(87,023; p=0.000)	2186 (46,9%) Khi-2(70,122; p=0.000)	78 (77,2%) Khi-2(51,828; p=0.000)	4604 (44,8%) Khi-2(109,628; p=0.000)	74 (79,6%) Khi-2(54,238; p=0.000)
Infection	8828(64,2%) Khi-2(518,198; p=0.000)	200(79,4%) Khi-2(35,369; p=0.000)	193 (80,1%) Khi-2(36583; p=0.000)	8153 (65,2%) Khi-2(57045; p=0.000)	184 (80,3%) Khi-2(36,397; p=0.000)	3260 (64%) Khi-2(24,575; p=0.000)	81 (77,9%) Khi-2(12,480; p=0.000)	7248 (66,1%) Khi-2(348,021; p=0.000)	76 (79,2%) Khi-2(13,329; p=0.000)
Fraude	450 (3,3%) Khi-2(6,084; p=0.048)	14 (5,6%) Khi-2(4,158; p=0.041)	13 (5,4%) Khi-2(34,33; p=0.061)	439 (3,5%) Khi-2(4,508; p=0.034)	11 (4,8%) Khi-2(1736; p=0.188)	176 (3,5%) Khi-2(1462; p=0.227)	7 (6,7%) Khi-2(112,957; p=0.000)	380 (3,5%) Khi-2(3973; p=0.046)	7 (7,3%) Khi-2(4948; p=0.026)

[80] Ont déclaré avoir un antivirus seulement (IRP_Q340)

[81] Ont déclaré avoir un pare-feu seulement(IRP_Q390_1)

[82] Ont déclaré supprimer les mails d'expéditeurs inconnus seulement (var : IRP_Q8380)

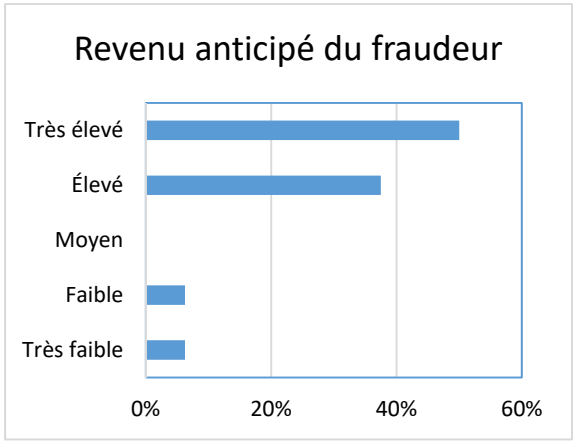
[83] Ont déclaré changer les mots de passe seulement (var : IRP_Q370)

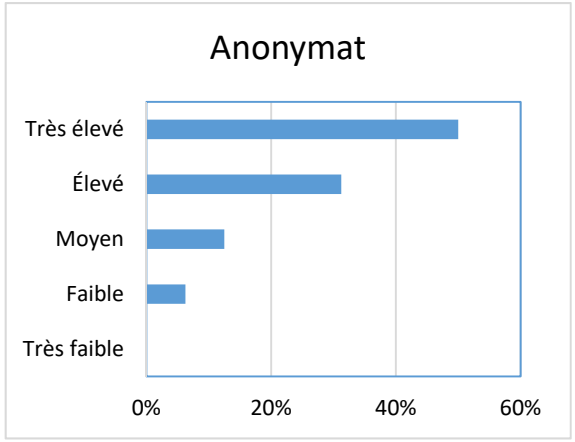
[84] Ont déclaré supprimer les fichiers temporaires (IRP_Q385)

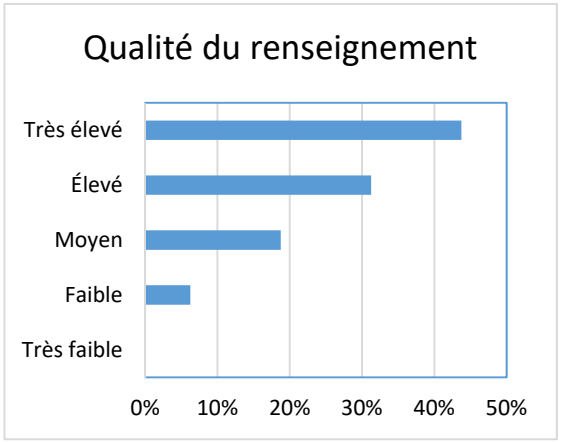
ANNEXE I : CODE MATLAB

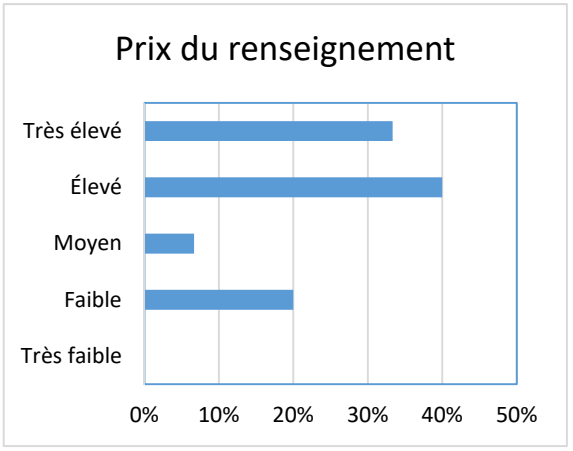
```
%initialisation des variables
syms r p R beta w a Q b k q qstarp dqdzp
syms X Y E Eprime E2prime Ux Uy qstar dqdz
%declaration des fonctions utilites
X=r +(R*(1-beta)*(1-W)*q)-a*Q-b
Y=r +(R*(1-beta)*(1-W)*q)-a*Q-b-(k*R*q)
%declaration des fonctions de risques
Ux=log(X)
Uy=log(Y)
%declaration de lesperence de gain
E=p*Ux+(1-p)*Uy
Eprime=diff(E,q)%derivee du premier ordre
% E2prime=diff(Eprime,beta)
qstar=solve(Eprime,q)%equation de la quantite de carte monetise obtenu de
lequation du premier odre
qstarp=subs(qstar,{Q,a,p,r,beta,W,b,k},{100,0.4,0.001,50,0.6,0.1,500,1})
figure(1)
ezplot(-qstarp,[500:1:10000])%le moin 1 signifie lajout de la constante Dq de
la condition du deuxieme ordre
ylabel('q')
qq=double(subs(-qstarp,[500:1:10000]));%extraire les donnes utiliser pour
tracer le graphe pour copier sur excel
figure(2)
% ezplot(Dqp,[0:0.01:1])
dqdz=(diff(qstar,R))
dqdzp=subs(dqdz,{r,beta,p,W,a,Q,b,k},{50,0.6,0.001,0.1,0.40,100,500,1})%la
derive de q* par rapport a R
```

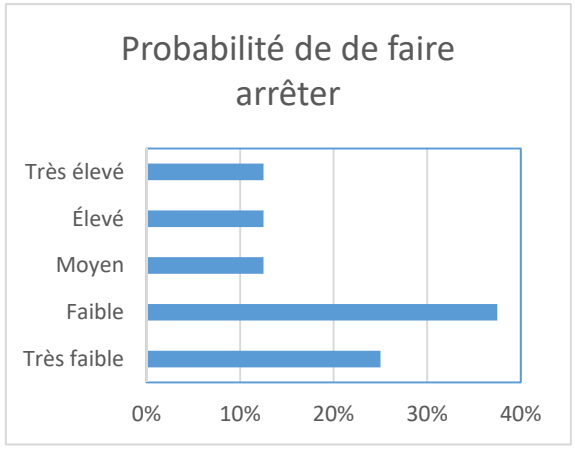
ANNEXE J : DEGRE D'ACCORD DES EXPERTS POUR CHAQUE FACTEUR DE MONETISATION

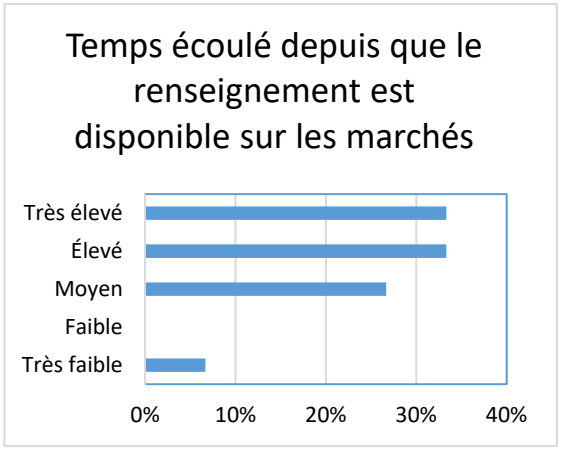


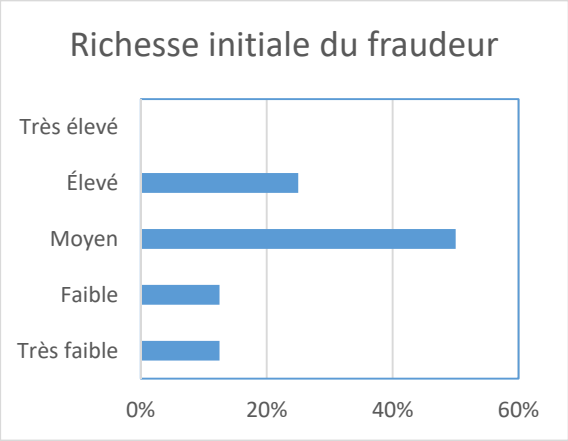


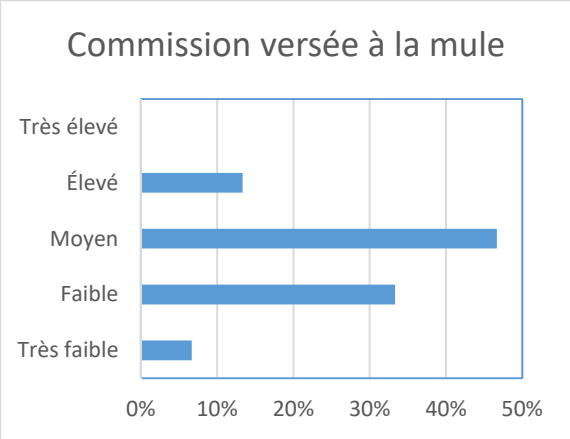


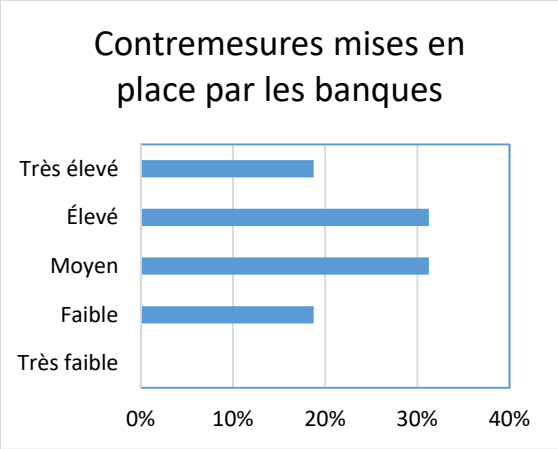







Richesse initiale du fraudeur
Très élevé
Élevé
Moyen
Faible
Très faible
0%
20%
40%
60%


Commission versée à la mule
Très élevé
Élevé
Moyen
Faible
Très faible
0%
10%
20%
30%
40%
50%


Contremesures mises en place par les banques
Très élevé
Élevé
Moyen
Faible
Très faible
0%
10%
20%
30%
40%

ANNEXE K : STATISTIQUES DESCRIPTIVES

Tableau K.1 : Avis d'experts sur les filtres anti-hameçonnage

#Experts	Meilleur réglage des critères de rejet	Signature numérique	Mécanismes d'empreinte avec authentification de l'émetteur	Formation de base en sécurité	Campagne de sensibilisation continue aux enjeux de sécurité
Exp1	3	3	3	2	2
Exp2	4	5	s/o	5	5
Exp3	3	4	2	5	5
Exp4	1	4	4	4	5
Exp5	5	1	1	5	5
Exp6	2	4	5	1	3
Exp7	4	5	3	5	5
Exp8	1	4	5	5	5
Exp9	4	3	4	5	5
Exp10	1	3	4	2	5
Exp11	1	5	4	2	2
Exp12	5	5	5	4	5
Exp13	3	4	5	4	3
Exp14	2	2	4	3	3
Exp15	3	1	3	2	2
Exp16	2	3	3	5	4
Exp17	3	4	4	2	2
Moyenne	2,76	3,53	3,69	3,59	3,88
Écart type	1,35	1,28	1,14	1,46	1,32
Total répondants / Échelle d'influence	N=17	N=17	N=16	N=17	N=17
Très faible	24%	12%	6%	6%	0%
Faible	18%	6%	6%	29%	24%
Moyen	29%	24%	25%	6%	18%
Forte	18%	35%	38%	18%	6%
Très forte	12%	24%	25%	41%	53%
	100%	100%	100%	100%	100%

Tableau K.2 : Avis d'experts sur les améliorations à apporter aux navigateurs

#Experts	Mise en place d'une barre d'outils standard pour les navigateurs	Mise en place d'un module standard de gestion des mots de passe	Adoption d'un navigateur standard pour toute l'organisation	Systèmes d'alerte anti-phishing actifs (intégrés) dans les navigateurs	Certificat EV SSL à validation étendue	Authentification multifactorielle
Exp1	2	2	1	4	3	5
Exp2	1	2	3	4	4	5
Exp3	3	3	3	4	4	3
Exp4	1	1	1	4	1	5
Exp5	2	5	5	5	2	5
Exp6	1	2	1	3	4	5
Exp7	3	4	4	4	4	5
Exp8	4	4	2	4	5	5
Exp9	3	4	2	2	2	5
Exp10	2	4	1		3	5
Exp11	4	3	1	4	3	2
Exp12	3	3	3	5	5	5
Exp13	2	3	3	4	4	5
Exp14	4	3	2	4	5	5
Exp15	4	4	4	4	3	3
Exp16	2	5	3	4	4	4
Exp17	s/o	2	2	3	3	4
Moyenne	2,6	3,2	2,4	3,9	3,5	4,5
Écart type	1,09	1,13	1,23	0,72	1,12	0,94
Total répondants / Échelle d'influence	N=16	N=17	N=17	N=16	N=17	N=17
Très faible	19%	6%	29%	0%	6%	0%
Faible	31%	24%	24%	6%	12%	6%
Moyen	25%	29%	29%	13%	29%	12%
Forte	25%	29%	12%	69%	35%	12%
Très forte	0%	12%	6%	13%	18%	71%
	100%	100%	100%	100%	100%	100%

Tableau K.3 : Avis d'experts sur les améliorations à apporter aux listes de restriction

#Experts	degré de satisfaction à l'égard du temps moyen de mise à jour de listes noires	degré de satisfaction à l'égard du temps moyen mise à jour de fichiers de journalisation au Canada	degré de satisfaction à l'égard du temps moyen mise à jour de fichiers de journalisation à l'étranger	votre degré de satisfaction à l'égard de la collaboration entre les partenaires - police	votre degré de satisfaction à l'égard de la collaboration entre pays	des solutions juridiques visant à favoriser l'échange des listes noires
Exp1	4	3	3		s/o	5
Exp2	3	4	4	1	1	s/o
Exp3	2	s/o	2	2	1	5
Exp4	s/o	s/o	s/o	1	1	1
Exp5	s/o	s/o	s/o	2	4	5
Exp6	4	5	5	s/o	s/o	s/o
Exp7	2	s/o	s/o	s/o	s/o	5
Exp8	1	s/o	s/o	s/o	2	4
Exp9	4	s/o	s/o	2	2	5
Exp10	3					
Exp11	3	3	3	1	1	4
Exp12	5	4	4	4	3	4
Exp13	3	2	1	3	2	3
Exp14	4	3	3	2	1	4
Exp15	2	2	2	s/o	s/o	s/o
Exp16	s/o	s/o	s/o	s/o	s/o	s/o
Exp17	4	3	s/o	3	2	4
Moyenne	3,14	3,22	3,00	2,10	1,82	4,08
Écart type	1,10	0,97	1,22	0,99	0,98	1,16
Total répondants / Échelle d'influence	N=14	N=9	N=9	N=10	N=11	N=12
Très faible	7%	0%	11%	30%	45%	8%
Faible	21%	22%	22%	40%	36%	0%
Moyen	29%	44%	33%	20%	9%	8%
Forte	36%	22%	22%	10%	9%	42%
Très forte	7%	11%	11%	0%	0%	42%
	100%	100%	100%	100%	100%	100%

Tableau K.4 : Avis d'experts sur la sécurisation de l'information lors des transactions

#Experts	Chiffrement des transactions	Témoins	Authentification de transaction en ligne par des protocoles suivants	Signature numérique
Exp1	5	3	3	2
Exp2	4	5	2	s/o
Exp3	5	4	3	4
Exp4	4	2	4	4
Exp5	5	4	4	1
Exp6	5	1	3	4
Exp7	3	5	4	5
Exp8	5	2	4	5
Exp9	1	3	3	3
Exp10				
Exp11	3	1	4	3
Exp12	5	3	5	5
Exp13	4	2	4	3
Exp14	5	2	3	2
Exp15	2	3	1	4
Exp16	4	4	4	2
Exp17	3	3	4	4
Moyenne	3,94	2,94	3,44	3,40
Écart type	1,24	1,24	0,96	1,24
Total répondants / Échelle d'influence	N=16	N=16	N=16	N=15
Très faible	6%	13%	6%	7%
Faible	6%	25%	6%	20%
Moyen	19%	31%	31%	20%
Forte	25%	19%	50%	33%
Très forte	44%	13%	6%	20%
	100%	100%	100%	100%

Tableau K.5 : Avis d'experts sur les formations et campagnes de sensibilisation contre les menaces

#Experts	Degré de satisfaction à l'égard de la formation anti-phishing individuelle	Degré de satisfaction à l'égard de la formation anti-phishing de groupe	Degré de satisfaction à l'égard des campagnes grand-public utilisant les réseaux sociaux	Degré de satisfaction à l'égard des développements des outils de formation
Exp1	3	3	3	3
Exp2	s/o	4	2	3
Exp3	2	2	1	3
Exp4	1	1	1	2
Exp5	4	3	2	3
Exp6	2	2	2	2
Exp7	4	4	4	2
Exp8	5	2	1	5
Exp9	4	s/o	2	s/o
Exp10		3	1	2
Exp11	2	1	2	
Exp12	3	3	3	3
Exp13	2	2	1	3
Exp14	4	4	3	4
Exp15	1	1	1	1
Exp16	3	2	2	2
Exp17	3	3	2	4
Moyenne	2,87	2,50	1,94	2,80
Écart type	1,19	1,03	0,90	1,01
Total répondants / Échelle d'influence	N=15	N=16	N=17	N=15
Très faible	13%	19%	35%	7%
Faible	27%	31%	41%	33%
Moyen	27%	31%	18%	40%
Forte	27%	19%	6%	13%
Très forte	7%	0%	0%	7%
	100%	100%	100%	100%

Tableau K.6 : Avis d'experts sur les facteurs qui influent sur le processus de monétisation

#Experts	Revenu	Probabilité	Richesse	Commission	Qualité	Temps écoulé	Niveaux des mesures	Anonymat	Prix
Exp1	5	4	3	2	3	4	2	4	4
Exp2	4	2	1		5	3	4	4	2
Exp3	4	2	3	2	4	5	5	4	5
Exp4	1	1	3	3	2	1	3	5	2
Exp5	5	1	3	3	5	5	5	2	2
Exp6	4	3	3	3	3	4	4	3	4
Exp7	5	5	3	2	4	4	4	5	5
Exp8	5	2	1	3	5	5	2	3	4
Exp9	5	2	2	3	4	3	3	4	4
Exp10	4	1	3	1	5	5	5	4	5
Exp11	2	1	4	4	4	3	3	5	4
Exp12									
Exp13	5	4	2	2	5	3	4	5	5
Exp14	4	3	4	2	3	4	3	5	3
Exp15	5	2	4	3	5	4	4	5	
Exp16	4	5	4	3	4	s/o	2	5	4
Exp17	5	2	3	4	5	5	3	5	5
Moyenne	4,2	2,5	2,9	2,7	4,1	3,9	3,5	4,3	3,9
Opinion de référence (criminologue)	5	1	3	3	5	5	5	2	2
Résultats de simulation du modèle théorique	5	1		5			5	1	1
Écart type	**1,17**	**1,37**		**0,96**	**0,82**	**0,96**	**1,13**	**1,03**	**0,93** **1,13**

Total répondants / Degré d'influence	Revenu N=16	Probabilité N=16	Richesse N=16	Commission N=15	Qualité N=16	Temps écoulé N=15	Niveaux des mesures N=16	Anonymat N=16	Prix N=15
Très faible	6%	25%	13%	7%	0%	7%	0%	0%	0%
Faible	6%	38%	13%	33%	6%	0%	19%	6%	20%
Moyen	0%	13%	50%	47%	19%	27%	31%	13%	7%
Forte	38%	13%	25%	13%	31%	33%	31%	31%	40%
Très forte	50%	13%	0%	0%	44%	33%	19%	50%	33%

ANNEXE L : ANALYSE DE VARIANCE -ANOVA-

Tableau L.1 : Effet de l'expérience des experts sur leurs choix des facteurs de monétisation

Revenu		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	,450	3	,150	,110	,952
	Intragroupes	9,550	7	1,364		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,552	3	1,517	1,279	,330
	Intragroupes	13,048	11	1,186		
	Total	17,600	14			
Probabilité		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	5,250	4	1,313	1,658	,276
	Intragroupes	4,750	6	,792		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,100	4	1,275	1,020	,443
	Intragroupes	12,500	10	1,250		
	Total	17,600	14			
Richesse		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,000	3	1,333	1,556	,283
	Intragroupes	6,000	7	,857		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,921	3	1,640	1,423	,288
	Intragroupes	12,679	11	1,153		
	Total	17,600	14			
Commission		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,733	3	,911	,886	,500
	Intragroupes	6,167	6	1,028		
	Total	8,900	9			

Tableau L.1 : Effet de l'expérience des experts sur leurs choix des facteurs de monétisation (suite)

Niveau d'expérience en sécurité informatique	Inter-groupes	3,881	3	1,294	,970	,445
	Intragroupes	13,333	10	1,333		
	Total	17,214	13			
Qualité du renseignement		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,500	3	,833	,778	,543
	Intragroupes	7,500	7	1,071		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	3,300	3	1,100	,846	,497
	Intragroupes	14,300	11	1,300		
	Total	17,600	14			
Delta-t		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	1,917	3	,639	,553	,662
	Intragroupes	8,083	7	1,155		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,850	4	1,463	1,245	,353
	Intragroupes	11,750	10	1,175		
	Total	17,600	14			
Niveau de mesures		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,800	3	,933	,907	,484
	Intragroupes	7,200	7	1,029		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,433	3	1,478	1,235	,344
	Intragroupes	13,167	11	1,197		
	Total	17,600	14			
Anonymat		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	1,600	2	,800	,762	,498
	Intragroupes	8,400	8	1,050		
	Total	10,000	10			

Tableau L.1 : Effet de l'expérience des experts sur leurs choix des facteurs de monétisation (suite et fin)

Niveau d'expérience en sécurité informatique	Inter-groupes	5,425	2	2,713	2,674	,110
	Intragroupes	12,175	12	1,015		
	Total	17,600	14			
Prix		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,667	3	1,556	2,042	,197
	Intragroupes	5,333	7	,762		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,300	3	1,433	1,280	,334
	Intragroupes	11,200	10	1,120		
	Total	15,500	13			

Tableau L.2 : Effet de l'expérience en sécurité informatique sur le choix des experts -filtre anti-hameçon-

Meilleur réglage des critères de rejet		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	8,667	4	2,167	9,750	,009
	Intragroupes	1,333	6	,222		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	7,117	4	1,779	1,519	,263
	Intragroupes	12,883	11	1,171		
	Total	20,000	15			
Signature numérique		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	8,000	4	2,000	6,000	,027
	Intragroupes	2,000	6	,333		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Intergroupes	7,167	4	1,792	1,536	,259
	Intragroupes	12,833	11	1,167		
	Total	20,000	15			
Mécanismes d'empreinte avec authentification de l'émetteur		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	1,567	3	,522	,427	,741
	Intragroupes	7,333	6	1,222		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Intergroupes	3,983	3	1,328	,927	,460
	Intragroupes	15,750	11	1,432		
	Total	19,733	14			

Tableau L.2 : Effet de l'expérience en sécurité informatique sur le choix des experts -filtre anti-hameçon-

(Suite et fin)

(Formation de base en sécurité		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,800	3	1,600	2,154	,182
	Intragroupes	5,200	7	,743		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	9,200	4	2,300	2,343	,119
	Intragroupes	10,800	11	,982		
	Total	20,000	15			
Campagne de sensibilisation continue aux enjeux de sécurité		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	5,619	2	2,810	5,130	,037
	Intragroupes	4,381	8	,548		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	9,000	3	3,000	3,273	,059
	Intragroupes	11,000	12	,917		
	Total	20,000	15			

Tableau L.3 : Effet de l'expérience en sécurité informatique sur le choix des experts -Navigateur-

Mise en place d'une barre d'outils standard pour les navigateurs		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	3,067	3	1,022	1,051	,436
	Intragroupes	5,833	6	,972		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,817	3	1,606	1,184	,360
	Intragroupes	14,917	11	1,356		
	Total	19,733	14			

Mise en place d'un module standard de gestion des mots de passe		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	6,000	4	1,500	2,250	,179
	Intragroupes	4,000	6	,667		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	7,000	4	1,750	1,481	,274
	Intragroupes	13,000	11	1,182		
	Total	20,000	15			

Adoption d'un navigateur standard pour toute l'organisation		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,583	4	,646	,522	,724
	Intragroupes	7,417	6	1,236		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	3,250	3	1,083	,776	,530
	Intragroupes	16,750	12	1,396		
	Total	20,000	15			

Tableau L.3 : Effet de l'expérience en sécurité informatique sur le choix des experts -Navigateur- (suite et fin)

Systèmes d'alerte anti-phishing intégrés et actifs dans les navigateurs		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,043	3	,681	,596	,641
	Intragroupes	6,857	6	1,143		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,597	3	1,866	1,452	,281
	Intragroupes	14,136	11	1,285		
	Total	19,733	14			
Certificat EV SSL à validation étendue		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,833	4	1,208	1,403	,338
	Intragroupes	5,167	6	,861		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	8,367	4	2,092	1,978	,168
	Intragroupes	11,633	11	1,058		
	Total	20,000	15			
Authentification multifactorielle		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,500	3	,833	,778	,543
	Intragroupes	7,500	7	1,071		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,318	3	1,773	1,449	,278
	Intragroupes	14,682	12	1,223		
	Total	20,000	15			

Tableau L.4 : Effet de l'expérience en sécurité informatique sur le choix des experts - Liste de restriction-

Degré de satisfaction à l'égard du temps moyen de MAJ liste noires		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,333	2	1,167	,913	,451
	Intragroupes	7,667	6	1,278		
	Total	10,000	8			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,550	4	1,388	1,255	,355
	Intragroupes	9,950	9	1,106		
	Total	15,500	13			
Degré de satisfaction à l'égard du temps moyen MAJ fichier de journalisation au Canada		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,450	1	2,450	2,673	,201
	Intragroupes	2,750	3	,917		
	Total	5,200	4			
Niveau d'expérience en sécurité informatique	Inter-groupes	6,889	3	2,296	5,741	,045
	Intragroupes	2,000	5	,400		
	Total	8,889	8			
Degré de satisfaction à l'égard du temps moyen MAJ fichier de journalisation à l'étranger		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,533	2	1,267	,950	,513
	Intragroupes	2,667	2	1,333		
	Total	5,200	4			
Niveau d'expérience en sécurité informatique	Inter-groupes	7,222	4	1,806	4,333	,092
	Intragroupes	1,667	4	,417		
	Total	8,889	8			

Tableau L.4 : Effet de l'expérience en sécurité informatique sur le choix des experts - Liste de restriction – (suite et fin)

Degré de satisfaction à l'égard de la collaboration entre les partenaires -police		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	3,667	3	1,222	1,351	,333
	Intragroupes	6,333	7	,905		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,810	4	1,452	1,126	,393
	Intragroupes	14,190	11	1,290		
	Total	20,000	15			

Degré de satisfaction à l'égard de la collaboration entre pays		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	1,200	3	,400	,312	,817
	Intragroupes	7,700	6	1,283		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	7,333	3	2,444	2,168	,149
	Intragroupes	12,400	11	1,127		
	Total	19,733	14			

Solutions juridiques visant à favoriser l'échange des listes noires		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	2,756	2	1,378	1,722	,256
	Intragroupes	4,800	6	,800		
	Total	7,556	8			
Niveau d'expérience en sécurité informatique	Inter-groupes	2,595	3	,865	,507	,690
	Intragroupes	11,950	7	1,707		
	Total	14,545	10			

Tableau L.5 : Effet de l'expérience en sécurité informatique sur le choix des experts -Transaction bancaire en ligne-

Chiffrement des transactions		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	3,650	3	1,217	1,390	,334
	Intragroupes	5,250	6	,875		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	5,400	4	1,350	,942	,479
	Intragroupes	14,333	10	1,433		
	Total	19,733	14			

Témoins		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,400	4	1,100	1,222	,406
	Intragroupes	4,500	5	,900		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	2,533	4	,633	,368	,826
	Intragroupes	17,200	10	1,720		
	Total	19,733	14			

Authentification de transaction en ligne par des protocoles 3D-Secure ou Verified By Visa et MasterCard SecureCode		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	1,900	2	,950	,950	,431
	Intragroupes	7,000	7	1,000		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	4,819	4	1,205	,808	,548
	Intragroupes	14,914	10	1,491		
	Total	19,733	14			

Tableau L.5 : Effet de l'expérience en sécurité informatique sur le choix des experts -Transaction bancaire en ligne- (suite et fin)

Signature numérique		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	4,389	4	1,097	1,386	,380
	Intragroupes	3,167	4	,792		
	Total	7,556	8			
Niveau d'expérience en sécurité informatique	Inter-groupes	6,629	3	2,210	1,726	,225
	Intragroupes	12,800	10	1,280		
	Total	19,429	13			

Tableau L.6 : Effet de l'expérience en sécurité informatique sur le choix des experts -formation et sensibilisation-

Degré de satisfaction à l'égard de la formation anti-phishing individuelle		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	,556	3	,185	,132	,937
	Intragroupes	7,000	5	1,400		
	Total	7,556	8			
Niveau d'expérience en sécurité informatique	Inter-groupes	8,762	4	2,190	1,848	,204
	Intragroupes	10,667	9	1,185		
	Total	19,429	13			

Degré de satisfaction à l'égard de la formation anti-phishing de groupe	Somme des carrés	ddl	Carré moyen	F	Sig.

Tableau L.6 : Effet de l'expérience en sécurité informatique sur le choix des experts -formation et sensibilisation- (suite et fin)

Niveau d'expérience en phishing	Inter-groupes	,900	3	,300	,225	,876
	Intragroupes	8,000	6	1,333		
	Total	8,900	9			
Niveau d'expérience en sécurité informatique	Inter-groupes	8,183	3	2,728	3,186	,067
	Intragroupes	9,417	11	,856		
	Total	17,600	14			

Degré de satisfaction à l'égard des campagnes grand-public utilisant les réseaux sociaux		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	3,200	3	1,067	1,098	,411
	Intragroupes	6,800	7	,971		
	Total	10,000	10			
Niveau d'expérience en sécurité informatique	Inter-groupes	1,667	3	,556	,364	,780
	Intragroupes	18,333	12	1,528		
	Total	20,000	15			

Degré de satisfaction à l'égard des développements des outils de formation		Somme des carrés	ddl	Carré moyen	F	Sig.
Niveau d'expérience en phishing	Inter-groupes	5,722	2	2,861	5,421	,045
	Intragroupes	3,167	6	,528		
	Total	8,889	8			
Niveau d'expérience en sécurité informatique	Inter-groupes	7,000	4	1,750	1,853	,203
	Intragroupes	8,500	9	,944		
	Total	15,500	13			